Microsoft CVE Summary

This report contains detail for the following vulnerabilities:

Tag	CVE ID	CVE Title	Severity
Azure CycleCloud	CVE-2024-43469	Azure CycleCloud Remote Code Execution Vulnerability	Important
Azure Network Watcher	CVE-2024-38188	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	Important
Azure Network Watcher	CVE-2024-43470	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	Important
Azure Stack	CVE-2024-38216	Azure Stack Hub Elevation of Privilege Vulnerability	Critical
Azure Stack	CVE-2024-38220	Azure Stack Hub Elevation of Privilege Vulnerability	Critical
Azure Web Apps	CVE-2024-38194	Azure Web Apps Elevation of Privilege Vulnerability	Critical
Dynamics Business Central	CVE-2024-38225	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	Important
Microsoft AutoUpdate (MAU)	CVE-2024-43492	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	Important
Microsoft Dynamics 365 (on-premises)	CVE-2024-43476	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important
Microsoft Graphics Component	CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2024-38250	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2024-38249	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Management Console	CVE-2024-38259	Microsoft Management Console Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-43465	Microsoft Excel Elevation of Privilege Vulnerability	Important
Microsoft Office Publisher	CVE-2024-38226	Microsoft Publisher Security Feature Bypass Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-38227	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-43464	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2024-38018	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2024-38228	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-43466	Microsoft SharePoint Server Denial of Service Vulnerability	Important
Microsoft Office Visio	CVE-2024-43463	Microsoft Office Visio Remote Code Execution Vulnerability	Important
Microsoft Outlook for iOS	CVE-2024-43482	Microsoft Outlook for iOS Information Disclosure Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38245	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38241	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38242	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important

Microsoft Streaming Service	CVE-2024-38244	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38243	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38237	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38238	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Power Automate	CVE-2024-43479	Microsoft Power Automate Desktop Remote Code Execution Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-38235	Windows Hyper-V Denial of Service Vulnerability	Important
SQL Server	CVE-2024-37338	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37980	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2024-26191	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37339	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37337	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-26186	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37342	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-43474	Microsoft SQL Server Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-37335	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37966	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-37340	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37965	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2024-37341	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
Windows Admin Center	CVE-2024-43475	Microsoft Windows Admin Center Information Disclosure Vulnerability	Important
Windows AllJoyn API	CVE-2024-38257	Microsoft AllJoyn API Information Disclosure Vulnerability	Important
Windows Authentication Methods	CVE-2024-38254	Windows Authentication Information Disclosure Vulnerability	Important
Windows DHCP Server	CVE-2024-38236	DHCP Server Service Denial of Service Vulnerability	Important
Windows Installer	CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	Important
Windows Kerberos	CVE-2024-38239	Windows Kerberos Elevation of Privilege Vulnerability	Important
Windows Kernel-Mode Drivers	CVE-2024-38256	Windows Kernel-Mode Driver Information Disclosure Vulnerability	Important
Windows Libarchive	CVE-2024-43495	Windows libarchive Remote Code Execution Vulnerability	Important

Windows Mark of the Web (MOTW)	CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	Important
Windows Mark of the Web (MOTW)	CVE-2024-43487	Windows Mark of the Web Security Feature Bypass Vulnerability	Moderate
Windows MSHTML Platform	CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	Important
Windows Network Address Translation (NAT)	CVE-2024-38119	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability	Critical
Windows Network Virtualization	CVE-2024-38232	Windows Networking Denial of Service Vulnerability	Important
Windows Network Virtualization	CVE-2024-38233	Windows Networking Denial of Service Vulnerability	Important
Windows Network Virtualization	CVE-2024-38234	Windows Networking Denial of Service Vulnerability	Important
Windows Network Virtualization	CVE-2024-43458	Windows Networking Information Disclosure Vulnerability	Important
Windows PowerShell	CVE-2024-38046	PowerShell Elevation of Privilege Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-38240	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38231	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38258	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43467	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43454	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38263	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38260	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43455	Windows Remote Desktop Licensing Service Spoofing Vulnerability	Important
Windows Security Zone Mapping	CVE-2024-30073	Windows Security Zone Mapping Security Feature Bypass Vulnerability	Important
Windows Setup and Deployment	CVE-2024-43457	Windows Setup and Deployment Elevation of Privilege Vulnerability	Important
Windows Standards-Based Storage Management Service	CVE-2024-38230	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	Important
Windows Storage	CVE-2024-38248	Windows Storage Elevation of Privilege Vulnerability	Important
Windows TCP/IP	CVE-2024-21416	Windows TCP/IP Remote Code Execution Vulnerability	Important
Windows TCP/IP	CVE-2024-38045	Windows TCP/IP Remote Code Execution Vulnerability	Important
Windows Update	CVE-2024-43491	Microsoft Windows Update Remote Code Execution Vulnerability	Critical
Windows Win32K - GRFX	CVE-2024-38246	Win32k Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-38252	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-38253	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important

CVE-2024-37338 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37338
MITRE
NVD</td><td>**CVE Title:** Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
Description:
Unknown
FAQ:

According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

I am running SQL Server on my system. What action do I need to take?

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

I am running my own application on my system. What action do I need to take?

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

I am running an application from a software vendor on my system. What action do I need to take?

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

• First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
• Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

• GDR updates – cumulatively only contain security updates for the given baseline.
• CU updates – cumulatively contain all functional fixes and security updates for the given baseline.</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	For any given baseline, either the GDR or CU updates could be options (see below). - If SQL Server installation is at a baseline version, you can choose either the GDR or CU update. - If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package. - If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package. **Note:** You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37338						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37338	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37966 - Microsoft SQL Server Native Scoring Information Disclosure Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37966
MITRE
NVD</td><td><b>CVE Title:</b> Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
<b>Description:</b>
Unknown
<b>FAQ:</b>

<b>According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?</b>

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

<b>What type of information could be disclosed by this vulnerability?</b>

An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.

<b>I am running SQL Server on my system. What action do I need to take?</b>

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

<b>I am running my own application on my system. What action do I need to take?</b>

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

<b>I am running an application from a software vendor on my system. What action do I need to take?</b>

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

<b>There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?</b>

• First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
• Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

<b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
</table>
</td><td>Important</td><td>Information Disclosure</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td></td><td>
<table>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>
<b>What are the GDR and CU update designations and how do they differ?</b>

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.
<ul>
<li>GDR updates – cumulatively only contain security updates for the given baseline.</li>
<li>CU updates – cumulatively contain all functional fixes and security updates for the given baseline.</li>
</ul>
For any given baseline, either the GDR or CU updates could be options (see below).
<ul>
<li>If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.</li>
<li>If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.</li>
<li>If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.</li>
</ul>
<b>Note:</b> You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

<b>Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?</b>

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

<b>Mitigations:</b>
None
<b>Workarounds:</b>
None
<b>Revision:</b>
1.0 2024-09-10T07:00:00

Information published.
</td><td></td><td></td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37966						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes

CVE-2024-37966						
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37966	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37335 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td></td><td>
<b>CVE Title:</b> Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<b>Description:</b>
Unknown
<b>FAQ:</b>

<b>According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?</b>

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

<b>I am running SQL Server on my system. What action do I need to take?</b>

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

<b>I am running my own application on my system. What action do I need to take?</b>

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

<b>I am running an application from a software vendor on my system. What action do I need to take?</b>

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

<b>There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?</b>

• First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
• Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

<b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
</table>
</td><td></td><td></td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37335
MITRE
NVD</td><td><table>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>
What are the GDR and CU update designations and how do they differ?
The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.
• GDR updates – cumulatively only contain security updates for the given baseline.
• CU updates – cumulatively contain all functional fixes and security updates for the given baseline.
For any given baseline, either the GDR or CU updates could be options (see below).
• If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
• If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
• If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.
Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.
Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?
Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.
Mitigations:
None
Workarounds:
None
Revision:
1.0   2024-09-10T07:00:00
Information published.</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

<table>
<tr><th colspan="8">CVE-2024-37335</th></tr>
<tr><th>Product</th><th>KB Article</th><th>Severity</th><th>Impact</th><th>Supersedence</th><th>CVSS Score Set</th><th>Restart Required</th></tr>
</table>

CVE-2024-37335						
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37335	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37340 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database. **I am running SQL Server on my system. What action do I need to take?** Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates. **I am running my own application on my system. What action do I need to take?** Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability. **I am running an application from a software vendor on my system. What action do I need to take?** Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability **There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?** - First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37340
MITRE
NVD</td><td>
<ul>
<li>determine the version, edition, and update level of SQL Server and its components.</li>
<li>Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.</li>
</ul>
<p><b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.</p>
<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>
<p><b>What are the GDR and CU update designations and how do they differ?</b></p>
<p>The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.</p>
<ul>
<li>GDR updates – cumulatively only contain security updates for the given baseline.</li>
<li>CU updates – cumulatively contain all functional fixes and security updates for the given baseline.</li>
</ul>
<p>For any given baseline, either the GDR or CU updates could be options (see below).</p>
<ul>
<li>If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.</li>
<li>If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.</li>
<li>If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.</li>
</ul>
<p><b>Note:</b> You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.</p>
<p><b>Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?</b></p>
<p>Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.</p>
<p><b>Mitigations:</b>
None
<b>Workarounds:</b>
None
<b>Revision:</b>
1.0   2024-09-10T07:00:00</p>
<p>Information published.</p>
</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37340						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37340	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37339 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database. **I am running SQL Server on my system. What action do I need to take?** Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates. **I am running my own application on my system. What action do I need to take?** Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability. **I am running an application from a software vendor on my system. What action do I need to take?** Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37339
MITRE
NVD</td><td>
vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

- First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

Mitigations:
None
Workarounds:
None
Revision:
1.0   2024-09-10T07:00:00

Information published.
</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37339						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37339	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37337 - Microsoft SQL Server Native Scoring Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Native Scoring Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database. **What type of information could be disclosed by this vulnerability?** An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37337
MITRE
NVD</td><td>

I am running SQL Server on my system. What action do I need to take?

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

I am running my own application on my system. What action do I need to take?

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

I am running an application from a software vendor on my system. What action do I need to take?

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

- First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

Mitigations:

</td><td>Important</td><td>Information Disclosure</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37337						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37337	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-37342 - Microsoft SQL Server Native Scoring Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Native Scoring Information Disclosure Vulnerability		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37342
MITRE
NVD</td><td><b>Description:</b>
Unknown
<b>FAQ:</b>

<b>According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?</b>

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

<b>What type of information could be disclosed by this vulnerability?</b>

An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.

<b>I am running SQL Server on my system. What action do I need to take?</b>

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

<b>I am running my own application on my system. What action do I need to take?</b>

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

<b>I am running an application from a software vendor on my system. What action do I need to take?</b>

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

<b>There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?</b>

• First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
• Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

<b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

<b>What are the GDR and CU update designations and how do they differ?</b>

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

• GDR updates – cumulatively only contain security updates for the given baseline.
• CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).</td><td>Important</td><td>Information Disclosure</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• If SQL Server installation is at a baseline version, you can choose either the GDR or CU update. • If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package. • If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package. **Note:** You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37342						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Information Disclosure	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37342	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-26186 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-26186
MITRE
NVD</td><td>

CVE Title: Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
Description:
Unknown
FAQ:

According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

I am running SQL Server on my system. What action do I need to take?

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

I am running my own application on my system. What action do I need to take?

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

I am running an application from a software vendor on my system. What action do I need to take?

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

- First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What are the GDR and CU update designations and how do they differ? The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release. - GDR updates – cumulatively only contain security updates for the given baseline. - CU updates – cumulatively contain all functional fixes and security updates for the given baseline. For any given baseline, either the GDR or CU updates could be options (see below). - If SQL Server installation is at a baseline version, you can choose either the GDR or CU update. - If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package. - If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package. **Note:** You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-26186						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-26186						
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-26186	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-26191 - Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

CVE Title: Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
Description:
Unknown
FAQ:

According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?

Successful exploitation of this vulnerability requires an authenticated attacker to leverage SQL Server Native Scoring to apply pre-trained models to their data without moving it out of the database.

I am running SQL Server on my system. What action do I need to take?

Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.

I am running my own application on my system. What action do I need to take?

Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.

I am running an application from a software vendor on my system. What action do I need to take?

Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

- First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

Update Number	Title	Apply if current product version is…	This security update also includes servicing releases up through…
5042578	Security update for SQL Server 2022 CU14+GDR	16.0.4003.1 - 16.0.4135.4	KB 5038325 - SQL2022 RTM CU14
5042211	Security update for SQL Server 2022 RTM+GDR	16.0.1000.6 - 16.0.1121.4	KB 5040936 - Previous SQL2022 RTM GDR

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-26191
MITRE
NVD</td><td>
<table>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

Mitigations:
None
Workarounds:
None
Revision:
1.0   2024-09-10T07:00:00

Information published.
</td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-26191						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-26191						
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-26191	Andrew Ruddick with Microsoft Security Response Center

CVE-2024-38018 - Microsoft SharePoint Server Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38018 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit the vulnerability?** In a network-based attack, an authenticated attacker, who has a minimum of Site Member permissions (PR:L), could execute code remotely on the SharePoint Server. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38018						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2024-38018						
Microsoft SharePoint Enterprise Server 2016	5002624 (Security Update)	Critical	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server 2019	5002639 (Security Update)	Critical	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server Subscription Edition	5002640 (Security Update)	Critical	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38018	Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative

CVE-2024-38216 - Azure Stack Hub Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38216 MITRE NVD	**CVE Title:** Azure Stack Hub Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, user interaction is required (UI:R) and privileges required are low (PR:L). What does that mean for this vulnerability?** An authenticated attacker must wait for a victim user to initiate a connection. **What privileges could an attacker gain with a successful exploitation?** An attacker who successfully exploited this vulnerability could gain unauthorized access to system resources, potentially allowing them to perform actions with the same privileges as the compromised process. This could lead to further system compromise and unauthorized actions within the network. **According to the CVSS metric, successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?** This vulnerability could lead to the attacker gaining the ability to interact with other tenant’s applications and content. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38216						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Stack Hub	Release Notes (Security Update)	Critical	Elevation of Privilege	None	Base: 8.2 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38216	Felix Boulet with Centre gouvernemental de cyberdéfense (CGCD) Mathieu Fiore Laroche with Centre gouvernemental de cyberdéfense (CGCD)

CVE-2024-38220 - Azure Stack Hub Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38220 MITRE NVD	**CVE Title:** Azure Stack Hub Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?** This vulnerability could lead to the attacker gaining the ability to interact with other tenant's applications and content. **What privileges could an attacker gain with a successful exploitation?** An attacker who successfully exploited this vulnerability could gain unauthorized access to system resources, potentially allowing them to perform actions with the same privileges as the compromised process. This could lead to further system compromise and unauthorized actions within the network. **According to the CVSS metric, user interaction is required (UI:R) and privileges required are low (PR:L). What does that mean for this vulnerability?** An authenticated attacker must wait for a victim user to initiate a connection. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38220						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Stack Hub	Release Notes (Security Update)	Critical	Elevation of Privilege	None	Base: 9.0 Temporal: 7.8 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38220	Mathieu Fiore Laroche with Centre gouvernemental de cyberdéfense (CGCD)

CVE-2024-38188 - Azure Network Watcher VM Agent Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38188 MITRE NVD	**CVE Title:** Azure Network Watcher VM Agent Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Is there any action I need to take to be protected from this vulnerability?** If you have enabled automatic updates, you will automatically receive the update as soon as it is available. If you have not enabled automatic updates, you will need to update the product manually. Please see Update Network Watcher extension to the latest version - Azure Virtual Machines | Microsoft Learn for more information. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploited this vulnerability could create, modify, or delete files in the security context of the NT AUTHORITY\SYSTEM account. **According to the CVSS metrics, successful exploitation of this vulnerability does nor impact confidentiality (C:N), but has major impact on integrity (I:H) and availability (A:H). What does that mean for this vulnerability?** Exploitation of this vulnerability does not disclose any confidential information but allows an attacker to modify or delete files containing data which could cause the service to become unavailable. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38188						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Network Watcher VM Extension for Windows	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38188	Filip Dragović

CVE-2024-38230 - Windows Standards-Based Storage Management Service Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38230 MITRE NVD	**CVE Title:** Windows Standards-Based Storage Management Service Denial of Service Vulnerability **Description:** Unknown **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38230						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38230						
installation)						
Windows Server 2019	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38230	k0shl with Kunlun Lab

CVE-2024-38236 - DHCP Server Service Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38236 MITRE NVD	**CVE Title:** DHCP Server Service Denial of Service Vulnerability **Description:** Unknown **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38236						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38236						
Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38236						
Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38236	Anonymous

CVE-2024-38240 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38240 MITRE NVD	**CVE Title:** Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38240						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38240						
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38240						
Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38240	George Hughey with MSRC Vulnerabilities & Mitigations

CVE-2024-38241 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38241 MITRE NVD	**CVE Title:** Kernel Streaming Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38241						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38241						
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38241						
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38241	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38242 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Kernel Streaming Service Driver Elevation of Privilege Vulnerability		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38242 MITRE NVD	**Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38242						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38242						
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38242						
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38242	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38249 - Windows Graphics Component Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38249 MITRE NVD	**CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38249						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38249						
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38249						
Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38249						
Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38249	Marcin Wiazowski working with Trend Micro Zero Day Initiative

CVE-2024-38250 - Windows Graphics Component Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38250 MITRE NVD	**CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38250						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office for Android	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Office for Universal	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-38250						
Microsoft Office LTSC for Mac 2021	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38250						
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38250						
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38250	Cristi Dudescu Cristi Dudescu Cristi Dudescu Cristi Dudescu

CVE-2024-38252 - Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38252 MITRE NVD	**CVE Title:** Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38252						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38252						
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38252						
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38252	Benjamin Rodes with Microsoft CodeQL George Hughey with MSRC Vulnerabilities & Mitigations

CVE-2024-38253 - Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38253 MITRE NVD	**CVE Title:** Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38253						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38253	George Hughey with MSRC Vulnerabilities & Mitigations Rohit Mothe with MSRC Vulnerabilities & Mitigations Benjamin Rodes with Microsoft CodeQL Devin Jensen

CVE-2024-38254 - Windows Authentication Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38254 MITRE NVD	**CVE Title:** Windows Authentication Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What type of information could be disclosed by this vulnerability?** An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38254						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38254						
10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based	5043080 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2024-38254						
Systems						
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38254	Rémi Jullian with Synacktiv

CVE-2024-38256 - Windows Kernel-Mode Driver Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38256 MITRE NVD	**CVE Title:** Windows Kernel-Mode Driver Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **What type of information could be disclosed by this vulnerability?** An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38256						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2024-38256						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Information Disclosure	None	Base: 5.5 Temporal: 4.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38256	Bùi Quang Hiếu (@tykawaii98)

CVE-2024-43463 - Microsoft Office Visio Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43463 MITRE NVD	**CVE Title:** Microsoft Office Visio Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** Exploitation of the vulnerability requires that a user open a specially crafted file. • In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. • In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43463						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft 365 Apps for Enterprise for 32-bit Systems	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft 365 Apps for Enterprise for 64-bit Systems	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office 2019 for 32-bit editions	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office 2019 for 64-bit editions	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 32-bit editions	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 64-bit editions	Click to Run (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Visio 2016 (32-bit edition)	5002634 (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-43463						
Microsoft Visio 2016 (64-bit edition)	5002634 (Security Update)	Important	Remote Code Execution	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43463	c0d3nh4ck with Zscaler's ThreatLabz

CVE-2024-43464 - Microsoft SharePoint Server Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43464 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is high (PR:H). What does that mean for this vulnerability?** An authenticated attacker with Site Owner permissions can use the vulnerability to inject arbitrary code and execute this code in the context of SharePoint Server. **How could an attacker exploit the vulnerability?** An authenticated attacker with Site Owner permissions or higher could upload a specially crafted file to the targeted SharePoint Server and craft specialized API requests to trigger deserialization of file's parameters. This would enable the attacker to perform remote code execution in the context of the SharePoint Server. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43464						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	5002624 (Security Update)	Critical	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server 2019	5002639 (Security Update)	Critical	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-43464						
Microsoft SharePoint Server Subscription Edition	5002640 (Security Update)	Critical	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43464	zcgonvh

CVE-2024-43467 - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43467 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to win a race condition. **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43467						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server						

CVE-2024-43467						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-43467						
Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43467	Lewis Lee Chunyang Han Zhiniang Peng

CVE-2024-43474 - Microsoft SQL Server Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **What type of information could be disclosed by this vulnerability?** An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory. **I am running SQL Server on my system. What action do I need to take?** Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates. **I am running my own application on my system. What action do I need to take?** Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability. **I am running an application from a software vendor on my system. What action do I need to take?** Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability **There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?** - First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-43474
MITRE
NVD</td><td>

- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

Mitigations:
None
Workarounds:
None
Revision:
1.0 2024-09-10T07:00:00

Information published.

</td><td>Important</td><td>Information Disclosure</td></tr>
</table>

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43474						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Information Disclosure	None	Base: 7.6 Temporal: 6.6 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Information Disclosure	None	Base: 7.6 Temporal: 6.6 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Information Disclosure	None	Base: 7.6 Temporal: 6.6 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43474	Anonymous

CVE-2024-43482 - Microsoft Outlook for iOS Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43482 MITRE NVD	**CVE Title:** Microsoft Outlook for iOS Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **How do I get the update for Outlook for IOS?** 1. Tap the Settings Icon 2. Tap the iTunes & App Store 3. Turn on AUTOMATIC DOWNLOADS for Apps **Alternatively** 1. Tap the App Store Icon 2. Scroll down to find Microsoft Outlook 3. Tap the Update button **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is file content. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43482						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Outlook for iOS	Release Notes (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43482	Masahiro Iida with LAC Co., Ltd.

CVE-2024-43492 - Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43492 MITRE NVD	**CVE Title:** Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **How can I find out what version of Teams I am running?** 1. Select the three dots (...) at the top right of the Teams window. 2. Select **Settings** 3. Select **About**, then **Version**. 4. The version will be displayed in a ribbon at the top of the Teams application. 5. You can get the latest version from the **Settings** menu by selecting **Check for updates**. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploits this vulnerability could elevate their privileges to perform commands as Root in the target environment. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43492						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft AutoUpdate for Mac	MAU (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43492	Anonymous

CVE-2024-43465 - Microsoft Excel Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43465 MITRE NVD	**CVE Title:** Microsoft Excel Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** Exploitation of the vulnerability requires that a user open a specially crafted file. • In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. • In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43465						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft 365 Apps for Enterprise for 32-bit Systems	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft 365 Apps for Enterprise for 64-bit Systems	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Excel 2016 (32-bit edition)	5002605 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Excel 2016 (64-bit edition)	5002605 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office 2019 for 64-bit editions	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 32-bit editions	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 64-bit editions	Click to Run (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC for Mac 2021	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Office Online Server	5002601 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43465	0x140ce

CVE-2024-37965 - Microsoft SQL Server Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft SQL Server Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **I am running SQL Server on my system. What action do I need to take?** Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates. **I am running my own application on my system. What action do I need to take?** Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability. **I am running an application from a software vendor on my system. What action do I need to take?**		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37965
MITRE
NVD</td><td>Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability

There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?

- First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
- Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.

<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

What privileges could be gained by an attacker who successfully exploited the vulnerability?

An attacker who successfully exploited this vulnerability could gain administrator privileges.

Mitigations:
None
Workarounds:
None
Revision:
1.0   2024-09-10T07:00:00</td><td>Important</td><td>Elevation of Privilege</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37965						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)	5042207 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack	5042209 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37965	Anonymous

CVE-2024-37341 - Microsoft SQL Server Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr>
<td>CVE-2024-37341
MITRE
NVD</td>
<td>
<p><b>CVE Title:</b> Microsoft SQL Server Elevation of Privilege Vulnerability
<b>Description:</b>
Unknown
<b>FAQ:</b></p>
<p><b>I am running SQL Server on my system. What action do I need to take?</b></p>
<p>Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.</p>
<p><b>I am running my own application on my system. What action do I need to take?</b></p>
<p>Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.</p>
<p><b>I am running an application from a software vendor on my system. What action do I need to take?</b></p>
<p>Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability</p>
<p><b>There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?</b></p>
<ul>
<li>First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.</li>
<li>Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.</li>
</ul>
<p><b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.</p>
<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
<tr><td>5042207</td><td>Security update for SQL Server 2016 SP3 RTM+GDR</td><td>13.0.6300.2 - 13.0.6441.1</td><td>KB 5040946 - Previous SQL2016 RTM GDR</td></tr>
</table>
<p><b>What are the GDR and CU update designations and how do they differ?</b></p>
<p>The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.</p>
<ul>
<li>GDR updates – cumulatively only contain security updates for the given baseline.</li>
<li>CU updates – cumulatively contain all functional fixes and security updates for the given baseline.</li>
</ul>
<p>For any given baseline, either the GDR or CU updates could be options (see below).</p>
<ul>
<li>If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.</li>
<li>If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.</li>
<li>If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.</li>
</ul>
<p><b>Note:</b> You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.</p>
<p><b>Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?</b></p>
<p>Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through</p>
</td>
<td>Important</td>
<td>Elevation of Privilege</td>
</tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploited this vulnerability could gain administrator privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37341						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)	5042207 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack	5042209 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37341	Anonymous

CVE-2024-38014 - Windows Installer Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38014 MITRE NVD	**CVE Title:** Windows Installer Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Detected	Not Found	N/A	No	Yes

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38014						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38014						
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38014						
Systems						
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38014						
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38014	Michael Baer with SEC Consult Vulnerability Lab

CVE-2024-38046 - PowerShell Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-	**CVE Title:** PowerShell Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could elevate their user privileges from those of a restrained user to an unrestrained WDAC user. **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
38046 MITRE NVD	The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38046						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38046						
Systems						
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38046						
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38046	Jimmy Bayne

CVE-2024-38217 - Windows Mark of the Web Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38217 MITRE NVD	**CVE Title:** Windows Mark of the Web Security Feature Bypass Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit the vulnerability?** To exploit this vulnerability, an attacker could host a file on an attacker-controlled server, then convince a targeted user to download and open the file. This could allow the attacker to interfere with the Mark of the Web functionality. Please see Additional information about Mark of the Web for further clarification **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, successful exploitation of this vulnerability could lead to some loss of integrity (I:L) and some loss of availability (A:L). What does that mean for this vulnerability?** An attacker can craft a malicious file that would evade Mark of the Web (MOTW) defenses, resulting in a limited loss of integrity and availability of security features such as SmartScreen Application Reputation security check and/or the legacy Windows Attachment Services security prompt. **Mitigations:** None **Workarounds:** None **Revision:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Detected	Not Found	N/A	Yes	Yes

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38217						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes

CVE-2024-38217						
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows						

CVE-2024-38217						
Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows						

CVE-2024-38217						
Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Security Feature Bypass	None	Base: 5.4 Temporal: 5.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:F/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38217	Joe Desimone with Elastic Security

CVE-2024-38225 - Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38225 MITRE NVD	**CVE Title:** Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit this vulnerability?** An attacker needs to edit the local configuration file to contain malicious code, then send the request to the server to exploit this vulnerability. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploited this vulnerability could gain administrator privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38225						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2024-38225						
Microsoft Dynamics 365 Business Central 2023 Release Wave 1	5042528 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Dynamics 365 Business Central 2023 Release Wave 2	5042530 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Dynamics 365 Business Central 2024 Release Wave 1	5042529 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38225	cjm00n with Cyber Kunlun & Zhiniang Peng

CVE-2024-38226 - Microsoft Publisher Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38226 MITRE NVD	**CVE Title:** Microsoft Publisher Security Feature Bypass Vulnerability **Description:** Unknown **FAQ:** **What kind of security feature could be bypassed by successfully exploiting this vulnerability?** An attacker who successfully exploited this vulnerability could bypass Office macro policies used to block untrusted or malicious files. **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **According to the CVSS metric, the attack vector is local (AV:L), privileges are required (PR:L) and user interaction is required (UI:R). How could an attacker exploit this security feature bypass vulnerability?** The attack itself is carried out locally by a user with authentication to the targeted system. An authenticated attacker could exploit the vulnerability by convincing a victim, through social engineering, to download and open a specially crafted file from a website which could lead to a local attack on the victim computer. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Security Feature Bypass

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Detected	Not Found	N/A	No	Yes

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38226						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-bit editions	Click to Run (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office 2019 for 64-bit editions	Click to Run (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 32-bit editions	Click to Run (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Office LTSC 2021 for 64-bit editions	Click to Run (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	No
Microsoft Publisher 2016 (32-bit edition)	5002566 (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft Publisher 2016 (64-bit edition)	5002566 (Security Update)	Important	Security Feature Bypass	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38226	None

CVE-2024-38227 - Microsoft SharePoint Server Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38227 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is high (PR:H). What does that mean for this vulnerability?** An authenticated attacker with Site Owner permissions can use the vulnerability to inject arbitrary code and execute this code in the context of SharePoint Server. **How could an attacker exploit the vulnerability?** An authenticated attacker with Site Owner permissions or higher could upload a specially crafted file to the targeted SharePoint Server and craft specialized API requests to trigger deserialization of file's parameters. This would enable the attacker to perform remote code execution in the context of the SharePoint Server. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38227						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	5002624 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server 2019	5002639 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server Subscription Edition	5002640 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38227	zcgonvh

CVE-2024-38228 - Microsoft SharePoint Server Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38228 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit the vulnerability?** An authenticated attacker with Site Owner permissions or higher could upload a specially crafted file to the targeted SharePoint Server and craft specialized API requests to trigger deserialization of file's parameters. This would enable the attacker to perform remote code execution in the context of the SharePoint Server. **According to the CVSS metric, privileges required is high (PR:H). What does that mean for this vulnerability?** An authenticated attacker with Site Owner permissions can use the vulnerability to inject arbitrary code and execute this code in the context of SharePoint Server. **Mitigations:** None **Workarounds:** None **Revision:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38228						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	5002624 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server 2019	5002639 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server Subscription Edition	5002640 (Security Update)	Important	Remote Code Execution	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38228	cjM00n & Edwardzpeng

CVE-2024-38231 - Windows Remote Desktop Licensing Service Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38231 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Denial of Service Vulnerability **Description:** Unknown **FAQ:** **Are there additional actions I need to take after I have installed the update?** No action is required from customers who are using a single license server and who are not using workgroup-joined Windows Server 2008 terminal servers. Customers using multiple license servers should refer to Use multiple remote desktop license servers for more information about the steps they need to take. Additionally, for proper license server discovery, customers using workgroup-joined Windows Server 2008 terminal servers will need to ensure that they list the RD license servers they want these terminal servers to use under **Use the specified Remote Desktop license servers** as detailed on this page. The License server discovery mode called "Automatically discover a license server" will no longer be supported in workgroup-joined deployment. **Mitigations:** None **Workarounds:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38231						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38231						
Windows Server 2012	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38231	Lewis Lee Chunyang Han Zhiniang Peng

CVE-2024-38232 - Windows Networking Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38232 MITRE NVD	**CVE Title:** Windows Networking Denial of Service Vulnerability **Description:** Unknown **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38232						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38232	Anonymous

CVE-2024-38233 - Windows Networking Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38233 MITRE NVD	**CVE Title:** Windows Networking Denial of Service Vulnerability **Description:** Unknown **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38233						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38233	Anonymous

CVE-2024-38234 - Windows Networking Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38234 MITRE NVD	**CVE Title:** Windows Networking Denial of Service Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack vector is adjacent (AV:A). What does that mean for this vulnerability?** An unauthenticated attacker with LAN access could exploit this vulnerability. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38234						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38234						
11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server						

CVE-2024-38234						
2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38234	Wei in Kunlun Lab with Cyber KunLun

CVE-2024-38235 - Windows Hyper-V Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38235 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, a successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?** Successful exploitation of this vulnerability could allow a Hyper-V guest to affect the functionality of the Hyper-V host. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38235						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38235						
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38235						
Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38235	Thunder_J with lichoin

CVE-2024-38237 - Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38237 MITRE NVD	**CVE Title:** Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38237						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2024-38237						
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38237						
11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38237	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38238 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38238 MITRE NVD	**CVE Title:** Kernel Streaming Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38238						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38238						
10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38238						
Systems						
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38238	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38239 - Windows Kerberos Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Windows Kerberos Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does this mean for this vulnerability?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38239 MITRE NVD	Successful exploitation of this vulnerability requires the attacker to have control over a domain controller and privileges to perform arbitrary code execution in a different trusted forest from the trusted forest containing the victim machine. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploited this vulnerability could gain domain administrator privileges. **According to the CVSS metric, privileges required is high (PR:H). What privileges are required to exploit this vulnerability?** The attacker needs to have privileges on the environment from where they are performing the attack and the environment they are targeting to be able to exploit this vulnerability. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38239						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38239						
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38239						
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38239						
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.2 Temporal: 6.3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38239	Microsoft Windows Authentication Team

CVE-2024-38243 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38243 MITRE NVD	**CVE Title:** Kernel Streaming Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38243						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38243						
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38243						
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38243	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38244 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38244 MITRE NVD	**CVE Title:** Kernel Streaming Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38244						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38244						
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38244	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38245 - Kernel Streaming Service Driver Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38245 MITRE NVD	**CVE Title:** Kernel Streaming Service Driver Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38245						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38245						
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38245						
Systems						
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38245						
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38245	Angelboy (@scwuaptx) with DEVCORE

CVE-2024-38246 - Win32k Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Win32k Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38246 MITRE NVD	**for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to win a race condition. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38246						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38246						
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38246	Cristi Dudescu Brent Mills

CVE-2024-38247 - Windows Graphics Component Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Windows Graphics Component Elevation of Privilege Vulnerability **Description:** Unknown		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38247 MITRE NVD	**FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38247						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38247						
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server						

CVE-2024-38247						
2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38247	Christopher Leung Christopher Leung

CVE-2024-38248 - Windows Storage Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38248 MITRE NVD	**CVE Title:** Windows Storage Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to win a race condition. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38248						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2024-38248						
Systems						
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows						

CVE-2024-38248						
Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Elevation of Privilege	None	Base: 7.0 Temporal: 6.3 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38248	lm0963 with TianGongLab of Legendsec at QI-ANXIN Group

CVE-2024-38257 - Microsoft AllJoyn API Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38257 MITRE NVD	**CVE Title:** Microsoft AllJoyn API Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38257						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version					Base: 7.5	

CVE-2024-38257						
1809 for ARM64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server					Base: 7.5	

CVE-2024-38257						
2016 (Server Core installation)	5043051 (Security Update)	Important	Information Disclosure	None	Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Information Disclosure	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38257	Cisco Talos

CVE-2024-38258 - Windows Remote Desktop Licensing Service Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38258 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is sensitive information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38258						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2024-38258						
Windows Server 2016	5043051 (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Information Disclosure	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38258	Chunyang Han Chunyang Han Zhiniang Peng

CVE-2024-38259 - Microsoft Management Console Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft Management Console Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38259 MITRE NVD	Exploitation of the vulnerability requires that a user open a specially crafted file. - In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. - In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38259						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38259						
Systems						
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38259	Anonymous

CVE-2024-38260 - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38260 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38260						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38260	Chunyang Han Zhiniang Peng Lewis Lee

CVE-2024-38263 - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38263 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to win a race condition. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38263						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server						

CVE-2024-38263						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38263						
Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38263	Lewis Lee Chunyang Han Zhiniang Peng

CVE-2024-21416 - Windows TCP/IP Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-21416 MITRE NVD	**CVE Title:** Windows TCP/IP Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to have a deep understanding of the system and the ability to manipulate its components to trigger a specific condition. Successful exploitation is not guaranteed and depends on a combination of factors that may include the environment, system configuration, and the presence of additional security measures. **How could an attacker exploit this vulnerability?** An attacker must send a specially crafted request to a Windows machine that has NetNAT service configured, which is a non-default configuration. In addition, specific network conditions must exist for exploitation to succeed. **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-21416						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-21416						
Systems						
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-21416	Wei in Kunlun Lab with Cyber KunLun

CVE-2024-38045 - Windows TCP/IP Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38045 MITRE NVD	**CVE Title:** Windows TCP/IP Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to have a deep understanding of the system and the ability to manipulate its components to trigger a specific condition. Successful exploitation is not guaranteed and depends on a combination of factors that may include the environment, system configuration, and the presence of additional security measures. **How could an attacker exploit this vulnerability?** An attacker must send a specially crafted request to a Windows machine that has NetNAT service configured, which is a non-default configuration. In addition, specific network conditions must exist for exploitation to succeed. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38045						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38045						
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38045						
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 8.1 Temporal: 7.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38045	Wei in Kunlun Lab with Cyber KunLun

CVE-2024-38119 - Windows Network Address Translation (NAT) Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38119 MITRE NVD	**CVE Title:** Windows Network Address Translation (NAT) Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires an attacker to win a race condition. **According to the CVSS metric, the attack vector is adjacent (AV:A). What does that mean for this vulnerability?** Successful exploitation of this vulnerability requires that an attacker will need to first gain access to the restricted network before running an attack. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38119						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-38119						
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-38119						
Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Critical	Remote Code Execution	None	Base: 7.5 Temporal: 6.5 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38119	Wei in Kunlun Lab with Cyber KunLun

CVE-2024-43454 - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43454 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, successful exploitation of this vulnerability could lead to some loss of availability (A:L) and a total loss of Integrity (I:H). What does that mean for this vulnerability?** Successful exploitation of this vulnerability enables an attacker to perform arbitrary file deletion (I:H). That file deletion might result in partial loss of component availability. (A:L). **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43454						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes

CVE-2024-43454						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes

CVE-2024-43454						
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.2 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43454	Chunyang Han Zhiniang Peng Lewis Lee

CVE-2024-43455 - Windows Remote Desktop Licensing Service Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43455 MITRE NVD	**CVE Title:** Windows Remote Desktop Licensing Service Spoofing Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit this vulnerability?** To successfully exploit this vulnerability an attacker must send specially crafted requests to the Terminal Server Licensing Service, which must be running and accessible over the network. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Spoofing

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43455						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-43455						
Windows Server 2016	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43455	Chunyang Han Zhiniang Peng Lewis Lee

CVE-2024-43457 - Windows Setup and Deployment Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43457 MITRE NVD	**CVE Title:** Windows Setup and Deployment Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What privileges could be gained by an attacker who successfully exploited this vulnerability?** An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43457						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Elevation of Privilege	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43457	Will Dormann with Vul Labs

CVE-2024-43458 - Windows Networking Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43458 MITRE NVD	**CVE Title:** Windows Networking Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **According to the CVSS metric, a successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?** Successful exploitation of this vulnerability could allow a Hyper-V guest to affect the functionality of the Hyper-V host. **Mitigations:** None **Workarounds:** None **Revision:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43458						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.7 Temporal: 6.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.7 Temporal: 6.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Information Disclosure	None	Base: 7.7 Temporal: 6.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43458	Anonymous

CVE-2024-43461 - Windows MSHTML Platform Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43461 MITRE NVD	**CVE Title:** Windows MSHTML Platform Spoofing Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **The Security Updates table indicates that this vulnerability affects all supported versions of Microsoft Windows. Why are IE Cumulative updates listed for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2?** While Microsoft has announced retirement of the Internet Explorer 11 application on certain platforms and the Microsoft Edge Legacy application is deprecated, the underlying MSHTML, EdgeHTML, and scripting platforms are still supported. The MSHTML platform is used by Internet Explorer mode in Microsoft Edge as well as other applications through WebBrowser control. The EdgeHTML platform is used by WebView and some UWP applications. The scripting platforms are used by MSHTML and EdgeHTML but can also be used by other legacy applications. Updates to	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	address vulnerabilities in the MSHTML platform and scripting engine are included in the IE Cumulative Updates; EdgeHTML and Chakra changes are not applicable to those platforms. To stay fully protected, we recommend that customers who install Security Only updates install the IE Cumulative updates for this vulnerability. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43461						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector:	Yes

CVE-2024-43461						
based Systems					CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for						

CVE-2024-43461						
32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043092 (Security Only) 5043049 (IE Cumulative)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes Maybe
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043092 (Security Only) 5043049 (IE Cumulative)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes Maybe
Windows Server 2012	5043125 (Monthly Rollup) 5043049 (IE Cumulative)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup) 5043049 (IE Cumulative)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server					Base: 8.8	

CVE-2024-43461						
2019 (Server Core installation)	5043050 (Security Update)	Important	Spoofing	None	Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Spoofing	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43461	Michael Macelletti, Naiyi Jiang and Adel with Microsoft Peter Girnus (@gothburz) of Trend Micro Zero Day Initiative

CVE-2024-43466 - Microsoft SharePoint Server Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43466 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Denial of Service Vulnerability **Description:** Unknown **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Denial of Service

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43466						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	5002624 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-43466						
Microsoft SharePoint Server 2019	5002639 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SharePoint Server Subscription Edition	5002640 (Security Update)	Important	Denial of Service	None	Base: 6.5 Temporal: 5.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43466	Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative

CVE-2024-43469 - Azure CycleCloud Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43469 MITRE NVD	**CVE Title:** Azure CycleCloud Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **How could an attacker exploit this vulnerability?** An attacker with basic user permissions can send specially crafted requests to modify the configuration of an Azure CycleCloud cluster to gain Root level permissions enabling them to execute commands on any Azure CycleCloud cluster in the current instance and in some scenarios, compromise administrator credentials. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43469						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure CycleCloud 8.0.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.0.1	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.0.2	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-43469						
Azure CycleCloud 8.1.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.1.1	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.2.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.2.1	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.2.2	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.3.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.4.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.4.1	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.4.2	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.5.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.6.0	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.6.1	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.6.2	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Azure CycleCloud 8.6.3	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43469	Anonymous

CVE-2024-43470 - Azure Network Watcher VM Agent Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Azure Network Watcher VM Agent Elevation of Privilege Vulnerability **Description:** Unknown **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43470 MITRE NVD	**Is there any action I need to take to be protected from this vulnerability?** If you have enabled automatic updates, you will automatically receive the update as soon as it is available. If you have not enabled automatic updates, you will need to update the product manually. Please see Update Network Watcher extension to the latest version - Azure Virtual Machines | Microsoft Learn for more information. **What privileges could be gained by an attacker who successfully exploited the vulnerability?** An attacker who successfully exploited this vulnerability could gain administrator privileges. **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** Exploitation of the vulnerability requires an admin user to stop or restart the service. **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43470						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Network Watcher VM Extension for Windows	Release Notes (Security Update)	Important	Elevation of Privilege	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43470	R4nger & Zhiniang Peng

CVE-2024-43475 - Microsoft Windows Admin Center Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE ID	**Vulnerability Description**	**Maximum Severity Rating**	**Vulnerability Impact**
CVE-2024-43475 MITRE NVD	**CVE Title:** Microsoft Windows Admin Center Information Disclosure Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** This attack requires a admin user on the client to connect to a malicious server and then take specific actions which could result in information disclosure. **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** The attacker must have permissions to access the target domain environment to be able to exploit this vulnerability. **What type of information could be disclosed by this vulnerability?** An attacker who successfully exploited this vulnerability could view heap memory from a privileged process running on the server. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Information Disclosure

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43475						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-43475						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Information Disclosure	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43475	Fangming Gu Qinghe Xie

CVE-2024-43476 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43476 MITRE NVD	**CVE Title:** Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** The user would have to navigate to a page with malicious content to be compromised by the attacker. **According to the CVSS metric, successful exploitation of this vulnerability could lead to some loss of integrity (I:L)? What does that mean for this vulnerability?** The attacker is only able to modify the content of the vulnerable link to redirect the victim to a malicious site. **According to the CVSS metric, a successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?** The vulnerability is in the web server, but the malicious scripts execute in the victim's browser on their machine. **According to the CVSS metric, privileges required is low (PR:L). What does that mean for this vulnerability?** Any authenticated attacker could trigger this vulnerability. It does not require admin or other elevated privileges. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Spoofing

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43476						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Dynamics 365 (on-premises) version 9.1	5043254 (Security Update)	Important	Spoofing	None	Base: 7.6 Temporal: 6.6 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43476	batram

CVE-2024-43479 - Microsoft Power Automate Desktop Remote Code Execution Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-43479
MITRE
NVD</td><td><b>CVE Title:</b> Microsoft Power Automate Desktop Remote Code Execution Vulnerability
<b>Description:</b>
Unknown
<b>FAQ:</b>
<b>According to the CVSS metrics, successful exploitation of this vulnerability could lead to major loss of confidentiality (C:H), integrity (I:H) and availability (A:H). What does that mean for this vulnerability?</b>
The attacker can execute arbitrary Desktop Flows scripts in the target user session by registering the machine to their own malicious Entra tenant, extracting the user's Sid, and creating a malicious AD domain with the same Sid. This allows them to mint valid Entra ID tokens that the attacked machine will trust to run desktop automation in the session of the user with the matching Sid.
<b>According to the CVSS metric, the attack complexity is high (AC:H). What does that mean for this vulnerability?</b>
Successful exploitation of this vulnerability requires an attacker to take additional actions prior to exploitation to prepare the target environment.
<b>According to the CVSS metric, a successful exploitation could lead to a scope change (S:C). What does this mean for this vulnerability?</b>
An attacker who successfully exploited this vulnerability could remotely execute arbitrary Desktop Flows script in an active open Windows session of the target user.
<b>How do I get the updated app?</b>
See Troubleshoot desktop flow action failures for update information.
<b>How can I check if the update is installed?</b>
Refer to the following table for the fixed build version that addresses this vulnerability.
<table>
<tr><th>If your current version is</th><th>Fixed build version</th></tr>
<tr><td>2.41</td><td>2.41.178.24249</td></tr>
<tr><td>2.42</td><td>2.42.331.24249</td></tr>
<tr><td>2.43</td><td>2.43.249.24249</td></tr>
</table></td><td>Important</td><td>Remote Code Execution</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2.44 2.44.55.24249 2.45 2.45.404.24249 2.46 2.46.181.24249 2.47 2.47.119.24249 **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.		

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43479						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Power Automate for Desktop	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: 8.5 Temporal: 7.4 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43479	Anonymous

CVE-2024-30073 - Windows Security Zone Mapping Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Windows Security Zone Mapping Security Feature Bypass Vulnerability **Description:** Unknown **FAQ:** **Windows 11, version 24H2 is not generally available yet. Why are there updates for this version of Windows listed in the Security Updates table?** The new Copilot+ devices that are now publicly available come with Windows 11, version 24H2 installed. Customers with these devices need to know about any vulnerabilities that affect their machine and to install the updates if they are not receiving automatic updates. Note that the general availability date for Windows 11, version 24H2 is scheduled for later this year. **What kind of security feature could be bypassed by successfully exploiting this vulnerability?** An URL path could be constructed by an attacker in such a way that the URL's Zone is interpreted as belonging to a more privileged zone		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-30073 MITRE NVD	**The Security Updates table indicates that this vulnerability affects all supported versions of Microsoft Windows. Why are IE Cumulative updates listed for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2?** While Microsoft has announced retirement of the Internet Explorer 11 application on certain platforms and the Microsoft Edge Legacy application is deprecated, the underlying MSHTML, EdgeHTML, and scripting platforms are still supported. The MSHTML platform is used by Internet Explorer mode in Microsoft Edge as well as other applications through WebBrowser control. The EdgeHTML platform is used by WebView and some UWP applications. The scripting platforms are used by MSHTML and EdgeHTML but can also be used by other legacy applications. Updates to address vulnerabilities in the MSHTML platform and scripting engine are included in the IE Cumulative Updates; EdgeHTML and Chakra changes are not applicable to those platforms. To stay fully protected, we recommend that customers who install Security Only updates install the IE Cumulative updates for this vulnerability. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Important	Security Feature Bypass

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-30073						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-30073						
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for ARM64-based Systems	5043067 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 version 21H2 for x64-based Systems	5043067 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for ARM64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 22H2 for x64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5043076 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for ARM64-based Systems	5043080 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 24H2 for x64-based Systems	5043080 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows						

CVE-2024-30073						
Server 2008 for 32-bit Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only) 5043049 (IE Cumulative)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	5043135 (Monthly Rollup) 5043087 (Security Only) 5043049 (IE Cumulative)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	5043135 (Monthly Rollup) 5043087 (Security Only)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	5043129 (Monthly Rollup) 5043092 (Security Only) 5043049 (IE Cumulative)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes Maybe
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	5043129 (Monthly Rollup) 5043092 (Security Only) 5043049 (IE Cumulative)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes Maybe
Windows Server 2012	5043049 (IE Cumulative) 5043125 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup) 5043049 (IE Cumulative)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	5043051 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-30073						
installation)						
Windows Server 2019	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022 (Server Core installation)	5042881 (Security Update) 5042880 (SecurityHotpatchUpdate)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5043055 (Security Update)	Important	Security Feature Bypass	None	Base: 7.8 Temporal: 6.8 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-30073	Anonymous

CVE-2024-43487 - Windows Mark of the Web Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43487 MITRE NVD	**CVE Title:** Windows Mark of the Web Security Feature Bypass Vulnerability **Description:** Unknown **FAQ:** **What kind of security feature could be bypassed by successfully exploiting this vulnerability?** An attacker who successfully exploited this vulnerability could bypass the SmartScreen user experience. **According to the CVSS metric, user interaction is required (UI:R). What interaction would the user have to do?** An attacker must send the user a malicious file and convince them to open it. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Moderate	Security Feature Bypass

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation More Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43487						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	5043083 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	5043051 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	5043051 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	5043050 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	5043050 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	5043050 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for 32-bit Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for ARM64-based Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 21H2 for x64-based Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 22H2 for 32-bit Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 22H2 for ARM64-based Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 22H2 for x64-based Systems	5043064 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012	5043125 (Monthly Rollup)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	5043125 (Monthly Rollup)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2	5043138 (Monthly Rollup)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes

CVE-2024-43487						
Windows Server 2012 R2 (Server Core installation)	5043138 (Monthly Rollup)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016	5043051 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	5043051 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2019	5043050 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	5043050 (Security Update)	Moderate	Security Feature Bypass	None	Base: 6.5 Temporal: 6.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:F/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43487	Mandar Sadye with Microsoft

CVE-2024-43491 - Microsoft Windows Update Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	CVE Title: Microsoft Windows Update Remote Code Execution Vulnerability **Description:** Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10, version 1507 (initial version released July 2015). This means that an attacker could exploit these previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability. This servicing stack vulnerability is addressed by installing the September 2024 Servicing stack update (SSU KB5043936) AND the September 2024 Windows security update (KB5043083), in that order. Note: Windows 10, version 1507 reached the end of support (EOS) on May 9, 2017 for devices running the Pro, Home, Enterprise, Education, and Enterprise IoT editions. Only Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB editions are still under support. **FAQ:** **How do I restore the fixes that this Windows Servicing Stack vulnerability rolled back?** Customers need to install both the servicing stack update (KB5043936) AND security update (KB5043083), released on September 10, 2024, to be fully protected from the vulnerabilities that this CVE rolled back. For more information see KB5043083. Customers whose systems are configured to receive automatic updates do not need to take any further action. **This CVE is marked as Exploitation Detected. Has Microsoft seen this vulnerability exploited in the wild?** This CVE documents the rollback of fixes that addressed vulnerabilities which affected some Optional Components for Windows 10 (version 1507). Some of these CVEs were known to be exploited, but no exploitation of CVE-2024-43491 itself has been detected. In addition, the Windows product team at Microsoft discovered this issue, and we have seen no evidence that it is publicly known.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43491 MITRE NVD	**Are there any actions I can take to prevent the rollback of previously fixed CVEs that this vulnerability caused?** No. If you have installed any of the previous security updates released between March and August 2024, the rollbacks of the fixes for CVEs affecting Optional Components have already occurred. To restore these fixes customers need to install the September 2024 Servicing Stack Update and Security Update for Windows 10. For more information see KB5043083. **Why were previously fixed CVEs rolled back?** Starting with the Windows security update released March 12, 2024 - KB5035858 (OS Build 10240.20526), the build version numbers crossed into a range that triggered a code defect in the Windows 10 (version 1507) servicing stack that handles the applicability of Optional Components. As a result, any Optional Component that was serviced with updates released since March 12, 2024 (KB5035858) was detected as "not applicable" by the servicing stack and was reverted to its RTM version. **Are all installations of Windows vulnerable?** No. Only Windows 10 (version 1507) (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) with Optional Components enabled from the following list are vulnerable. All other versions of Windows 10 released since November 2015 are not affected. • .NET Framework 4.6 Advanced Services \ ASP.NET 4.6 • Active Directory Lightweight Directory Services • Administrative Tools • Internet Explorer 11 • Internet Information Services\World Wide Web Services • LPD Print Service • Microsoft Message Queue (MSMQ) Server Core • MSMQ HTTP Support • MultiPoint Connector • SMB 1.0/CIFS File Sharing Support • Windows Fax and Scan • Windows Media Player • Work Folders Client • XPS Viewer **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Detected	Not Found	N/A	No	Yes

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43491						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	5043083 (Security Update)	Critical	Remote Code Execution	None	Base: 9.8 Temporal: 8.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-43491						
Windows 10 for x64-based Systems	5043083 (Security Update)	Critical	Remote Code Execution	None	Base: 9.8 Temporal: 8.5 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43491	Anonymous

CVE-2024-43495 - Windows libarchive Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-43495 MITRE NVD	**CVE Title:** Windows libarchive Remote Code Execution Vulnerability **Description:** Unknown **FAQ:** **According to the CVSS metric, the attack vector is local (AV:L). Why does the CVE title indicate that this is a remote code execution?** The word **Remote** in the title refers to the location of the attacker. This type of exploit is sometimes referred to as Arbitrary Code Execution (ACE). The attack itself is carried out locally. This means an attacker or victim needs to execute code from the local machine to exploit the vulnerability. **According to the CVSS metric, user interaction is required (UI:R) and privileges required is low (PR:L). What does that mean for this vulnerability?** An authenticated attacker with guest privileges must send the victim a malicious RAR file and convince them to open it. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published. This CVE was addressed by updates that were released in July 2024, but the CVE was inadvertently omitted from the July 2024 Security Updates. This is an informational change only. Customers who have already installed the July 2024 updates do not need to take any further action.	Important	Remote Code Execution

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-43495						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 11 Version 22H2 for ARM64-based Systems	5040442 (Security Update)	Important	Remote Code Execution	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2024-43495						
Windows 11 Version 22H2 for x64-based Systems	5040442 (Security Update)	Important	Remote Code Execution	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for ARM64-based Systems	5040442 (Security Update)	Important	Remote Code Execution	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 11 Version 23H2 for x64-based Systems	5040442 (Security Update)	Important	Remote Code Execution	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2022, 23H2 Edition (Server Core installation)	5040438 (Security Update)	Important	Remote Code Execution	None	Base: 7.3 Temporal: 6.4 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-43495	wh1tc & Zhiniang Peng HAO LI with Venustech ADLab

CVE-2024-38194 - Azure Web Apps Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2024-38194 MITRE NVD	**CVE Title:** Azure Web Apps Elevation of Privilege Vulnerability **Description:** An authenticated attacker can exploit an improper authorization vulnerability in Azure Web Apps to elevate privileges over a network. **FAQ:** **Why are there no links to an update or instructions with steps that must be taken to protect from this vulnerability?** This vulnerability has already been fully mitigated by Microsoft. There is no action for users of this service to take. This purpose of this CVE is to provide further transparency. Please see Toward greater transparency: Unveiling Cloud Service CVEs for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2024-09-10T07:00:00 Information published.	Critical	Elevation of Privilege

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-38194						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Web Apps		Critical	Elevation of Privilege	None	Base: 8.4 Temporal: 7.3 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:U/RL:O/RC:C	Unknown

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-38194	Shimi Gersner with Azure Networking Security Research (ANSR), Microsoft

CVE-2024-37980 - Microsoft SQL Server Elevation of Privilege Vulnerability

(top)

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td>CVE-2024-37980
MITRE
NVD</td><td>
<b>CVE Title:</b> Microsoft SQL Server Elevation of Privilege Vulnerability
<b>Description:</b>
Unknown
<b>FAQ:</b>
<p><b>I am running SQL Server on my system. What action do I need to take?</b></p>
<p>Update your relevant version of SQL Server. Any applicable driver fixes are included in those updates.</p>
<p><b>I am running my own application on my system. What action do I need to take?</b></p>
<p>Update your application to use Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed on this page, which provide protection against this vulnerability.</p>
<p><b>I am running an application from a software vendor on my system. What action do I need to take?</b></p>
<p>Consult with your application vendor if it is compatible with Microsoft OLE DB Driver 18 or 19. Update the drivers to the versions listed in this page, which provide protection against this vulnerability</p>
<p><b>There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?</b></p>
<ul>
<li>First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.</li>
<li>Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.</li>
</ul>
<p><b>Note</b> If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.</p>
<table>
<tr><th>Update Number</th><th>Title</th><th>Apply if current product version is…</th><th>This security update also includes servicing releases up through…</th></tr>
<tr><td>5042578</td><td>Security update for SQL Server 2022 CU14+GDR</td><td>16.0.4003.1 - 16.0.4135.4</td><td>KB 5038325 - SQL2022 RTM CU14</td></tr>
<tr><td>5042211</td><td>Security update for SQL Server 2022 RTM+GDR</td><td>16.0.1000.6 - 16.0.1121.4</td><td>KB 5040936 - Previous SQL2022 RTM GDR</td></tr>
<tr><td>5042749</td><td>Security update for SQL Server 2019 CU28+GDR</td><td>15.0.4003.23 - 15.0.4385.2</td><td>KB 5039747 - SQL2019 RTM CU28</td></tr>
<tr><td>5042214</td><td>Security update for SQL Server 2019 RTM+GDR</td><td>15.0.2000.5 - 15.0.2116.2</td><td>KB 5040986 - Previous SQL2019 RTM GDR</td></tr>
<tr><td>5042215</td><td>Security update for SQL Server 2017 CU31+GDR</td><td>14.0.3006.16 - 14.0.3471.2</td><td>KB 5040940 - SQL2017 RTM CU31</td></tr>
<tr><td>5042217</td><td>Security update for SQL Server 2017 RTM+GDR</td><td>14.0.1000.169 - 14.0.2056.2</td><td>KB 5040942 - Previous SQL2017 RTM GDR</td></tr>
<tr><td>5042209</td><td>Security update for SQL 2016 Azure Connect Feature Pack</td><td>13.0.7000.253 - 13.0.7037.1</td><td>KB 5040944 - SQL2016 Azure Connect Feature Pack</td></tr>
</table>
</td><td>Important</td><td>Elevation of Privilege</td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

5042207	Security update for SQL Server 2016 SP3 RTM+GDR	13.0.6300.2 - 13.0.6441.1	KB 5040946 - Previous SQL2016 RTM GDR

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?

Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.

What privileges could be gained by an attacker who successfully exploited the vulnerability?

An attacker who successfully exploited this vulnerability could gain administrator privileges.

Mitigations:
None
Workarounds:
None
Revision:
1.0 2024-09-10T07:00:00

Information published.

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Publicly Disclosed	Exploited
Exploitation Less Likely	Not Found	N/A	No	No

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2024-37980						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)	5042207 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack	5042209 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe

CVE-2024-37980						
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	5042215 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	5042217 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Maybe
Microsoft SQL Server 2019 for x64-based Systems (CU 28)	5042749 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2019 for x64-based Systems (GDR)	5042214 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (CU 14)	5042578 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Microsoft SQL Server 2022 for x64-based Systems (GDR)	5042211 (Security Update)	Important	Elevation of Privilege	None	Base: 8.8 Temporal: 7.7 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

Acknowledgements

CVE ID	Acknowledgements
CVE-2024-37980	Anonymous