Microsoft

Microsoft Security Release

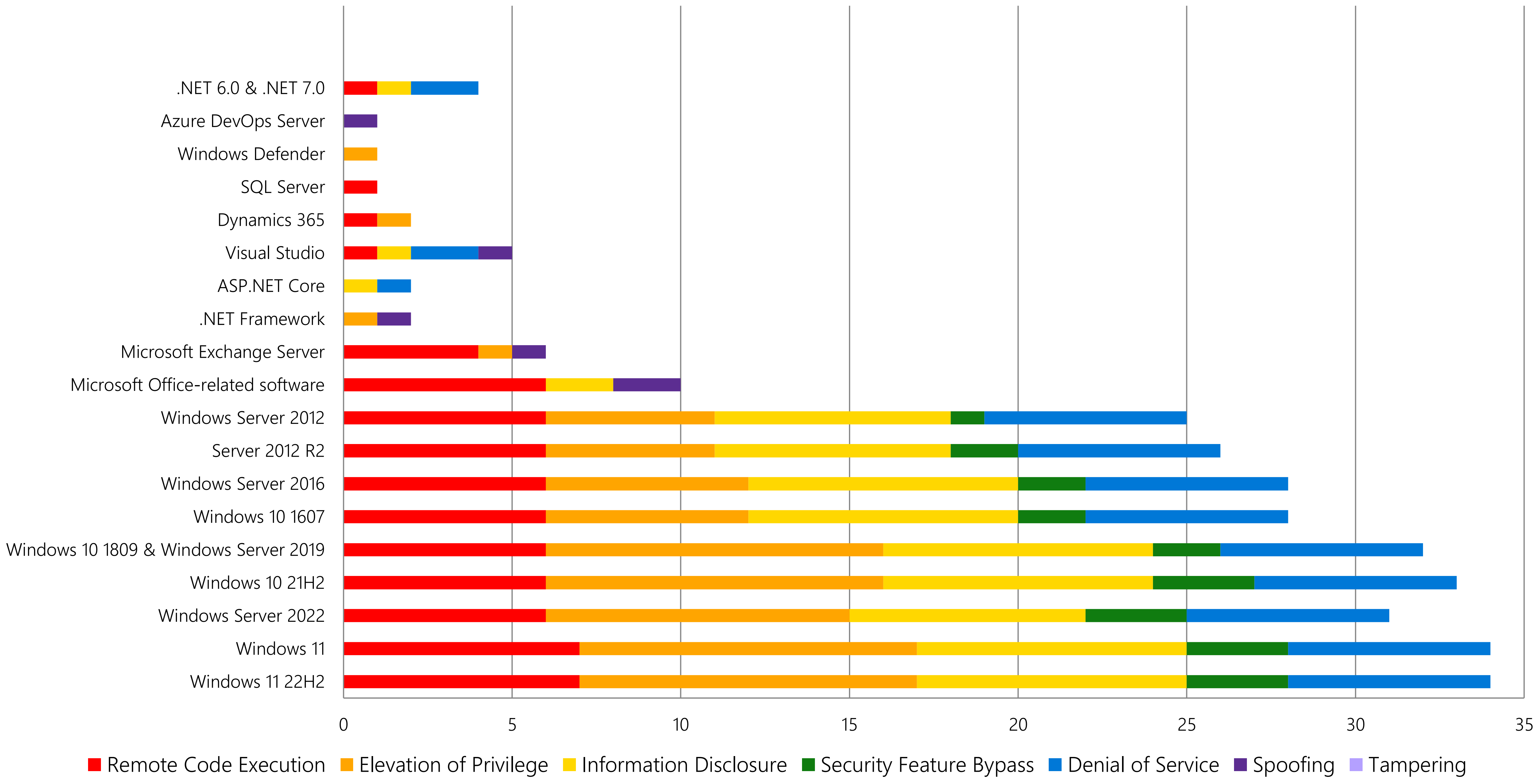
August 8, 2023

Agenda

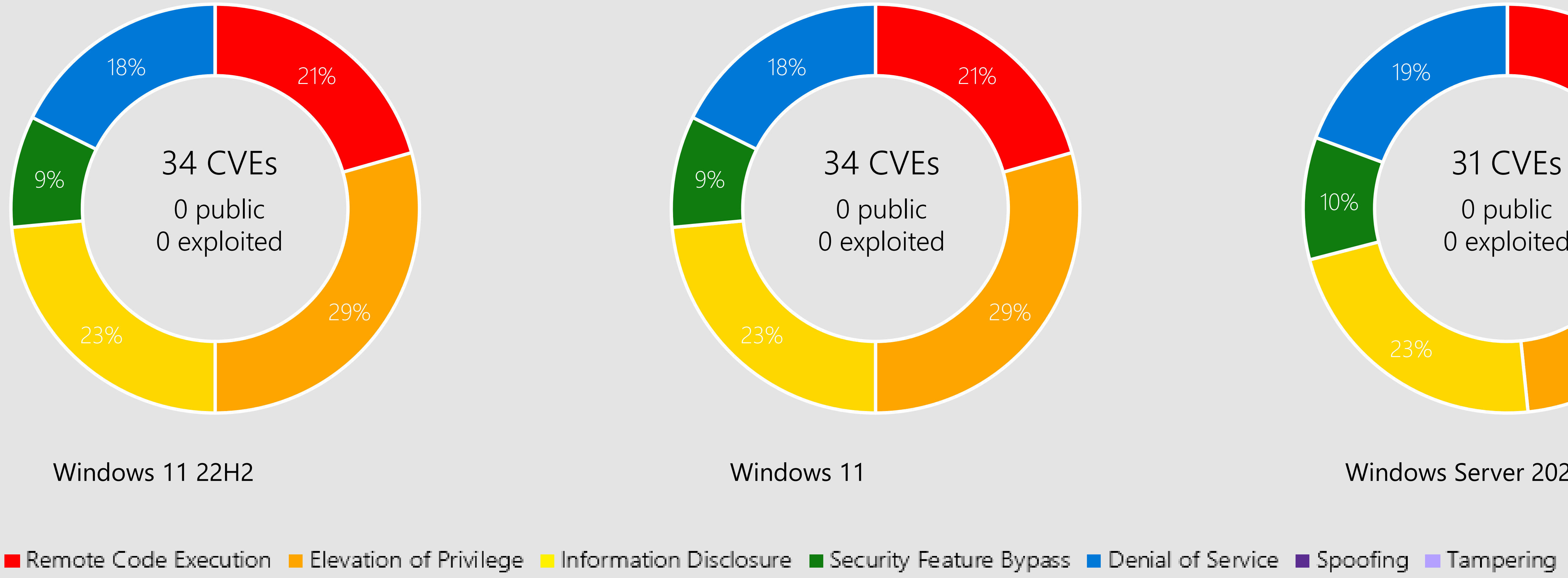
- Security Updates
- Security Advisories
- Product Support Lifecycle
- Other resources related to the release

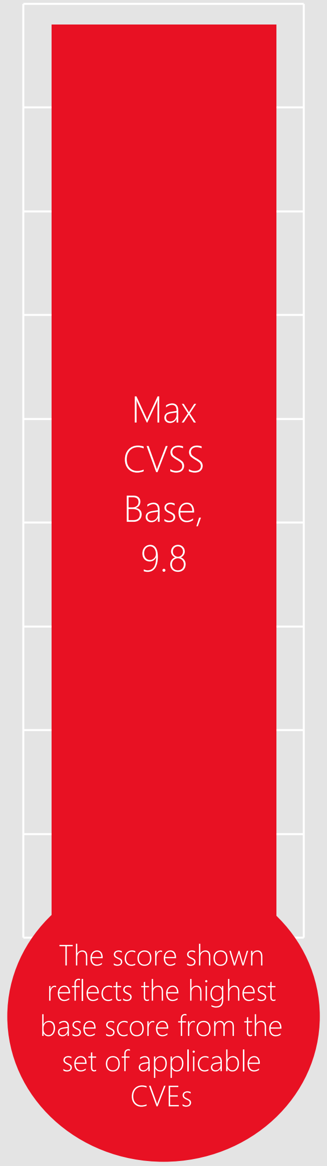
Monthly Security Release Overview - August 2023

Vulnerabilities fixed by component and by impact



Windows 11, Server 2022





The score shown reflects the highest base score from the set of applicable CVEs

Affected Components:

- Bluetooth A2DP driver
- Cloud Files Mini Filter Driver
- Projected File System
- CLFS Driver
- Cryptographic Services
- Fax Service
- Group Policy
- HTML Platforms
- Hyper-V
- Kernel
- LDAP
- Message Queuing
- MDM
- Smart Card Resource Management Server
- System Assessment Tool
- Tablet User Interface Application Core
- WDAC OLE DB provider for SQL Server

SA230003 Microsoft Office Defense in Depth Update

Summary

This defense in depth update is not a vulnerability, but installing this update stops the attack chain leading to the Windows Search security feature bypass vulnerability (CVE-2023-36884). Microsoft recommends installing this update as well as applying the August 2023 updates for Windows.

Recommended Actions:

1. Apply the August Office updates
2. Apply the August Windows updates

CVE-2023-36910 Message Queuing

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 9.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

The Windows message queuing service, which is a Windows component, needs to be enabled for a system to be exploitable by this vulnerability. This feature can be added via the Control Panel. You can check to see if there is a service running named Message Queuing and TCP port 1801 is listening on the machine.

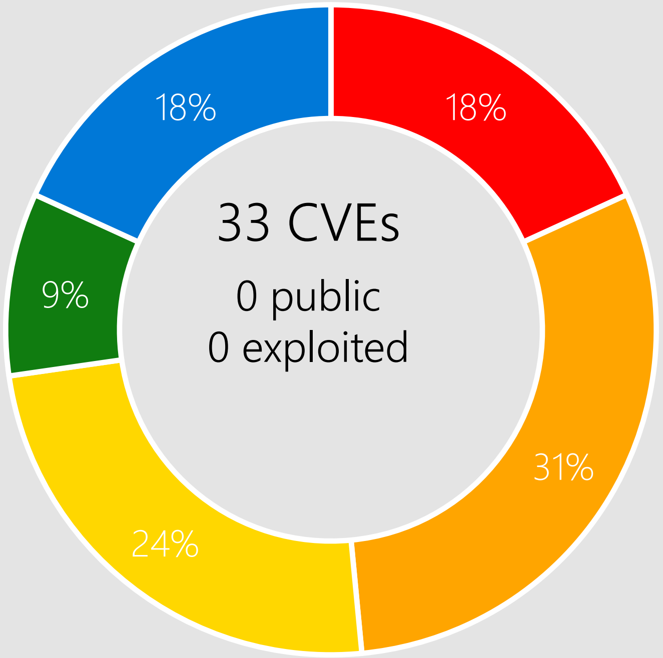
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

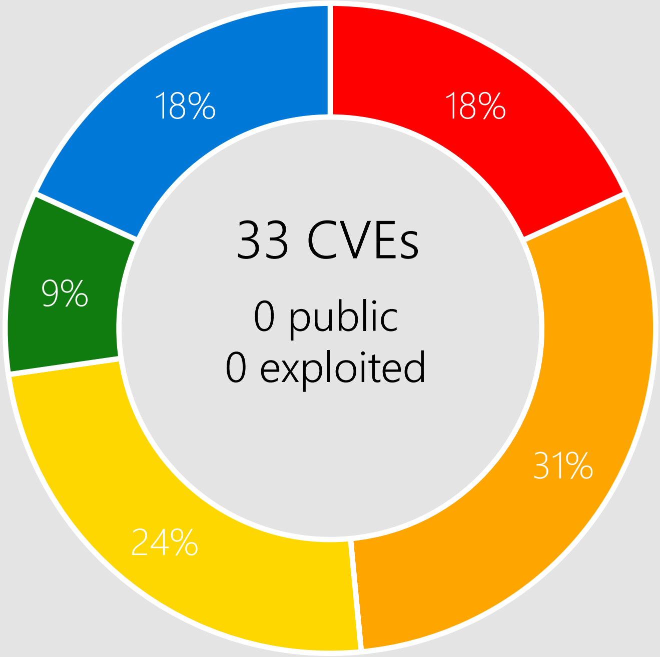
Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

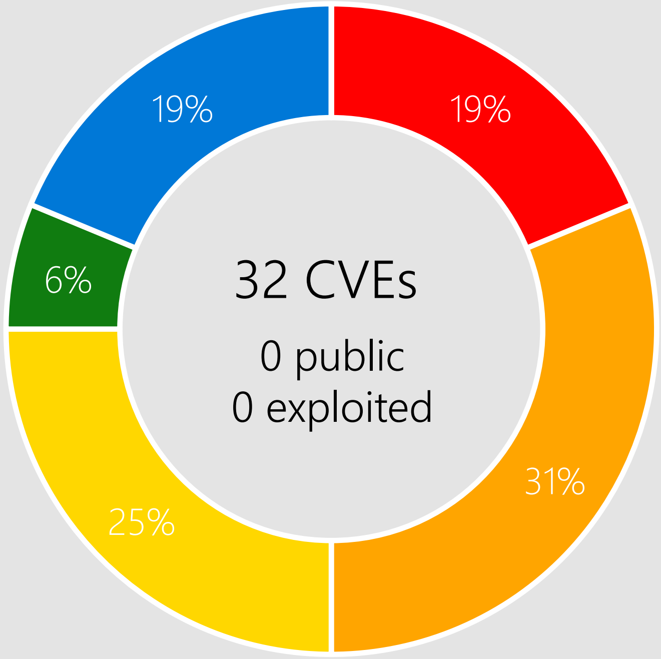
Windows 10



Windows 10 22H2

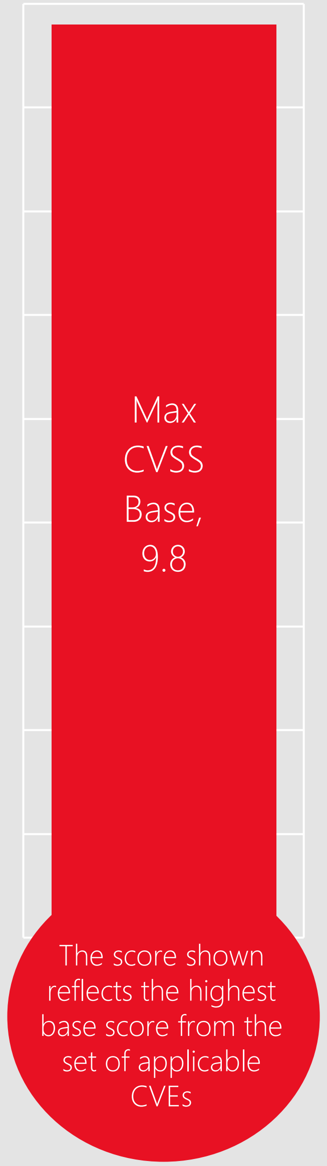


Windows 10 21H2



Windows 10 1809 & Windows Server 2019

🟥 Remote Code Execution 🟧 Elevation of Privilege 🟨 Information Disclosure 🟩 Security Feature Bypass 🟦 Denial of Service 🟪 Spoofing 🟪 Tampering



Max CVSS Base, 9.8

The score shown reflects the highest base score from the set of applicable CVEs

Affected Components:

Bluetooth A2DP driver
Cloud Files Mini Filter Driver
Projected File System

CLFS Driver
Cryptographic Services
Fax Service

Group Policy
HTML Platforms
Hyper-V

Kernel
LDAP
Message Queuing

MDM
Smart Card Resource Management Server
System Assessment Tool

WDAC OLE DB provider for SQL Server
WwanSvc

CVE-2023-35381 Fax Service

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

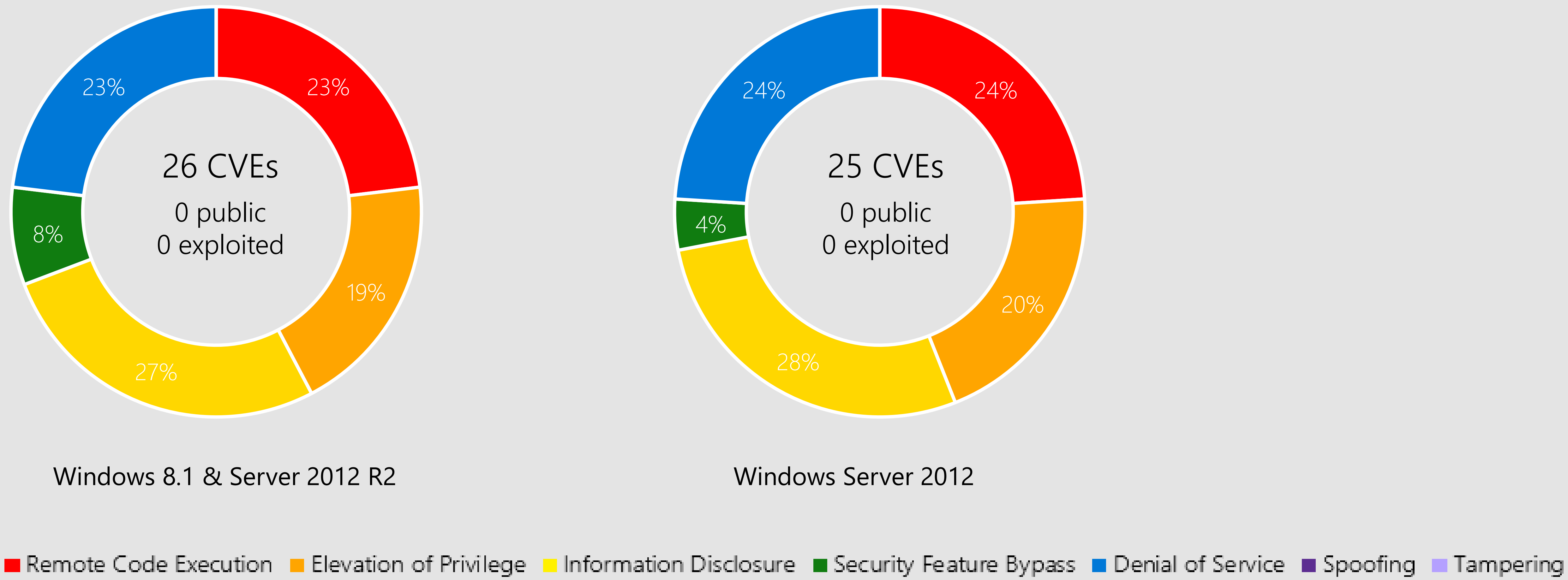
Workarounds

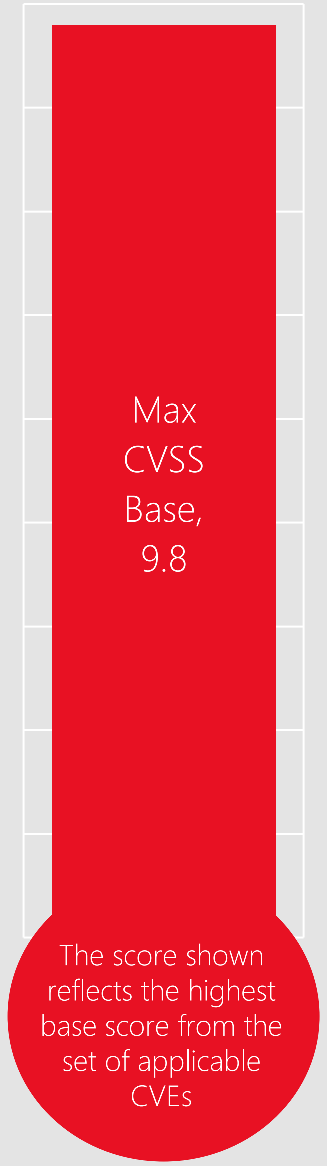
Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

Server 2012 R2, and Server 2012





The score shown reflects the highest base score from the set of applicable CVEs

Affected Components:

Bluetooth A2DP driver
CLFS Driver
Cryptographic Services
Fax Service
Group Policy
HTML Platforms
Hyper-V
Kernel
LDAP
Message Queuing
System Assessment Tool

CVE-2023-35387 Bluetooth A2DP Driver

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

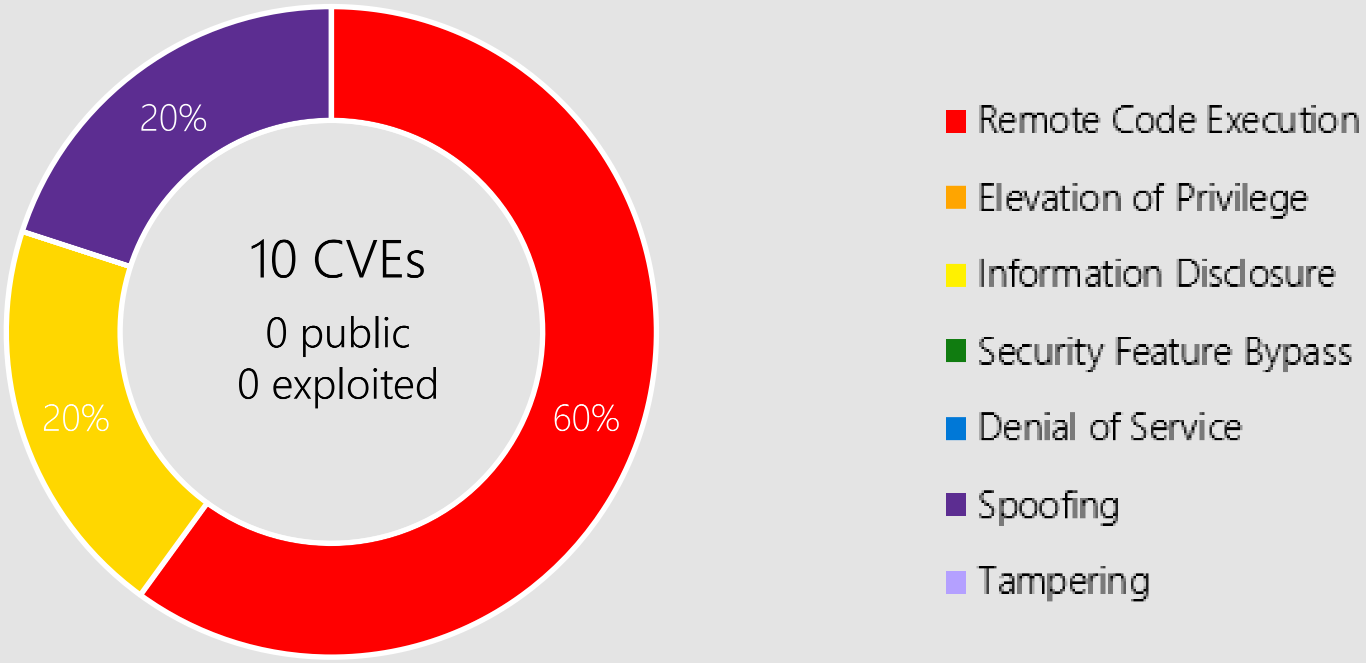
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Word 2013/2016
Outlook 2013/2016
Excel 2013/2016
PowerPoint 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Project 2013
Project 2016
Publisher 2013
Publisher 2016
SharePoint Server Subscription Edition
Teams Android
Teams Desktop
Teams for Mac
Teams iOS
Visio 2013
Visio 2016

CVE-2023-29328 Microsoft Teams

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Microsoft Teams for Desktop
Microsoft Teams for iOS
Microsoft Teams for Android
Microsoft Teams for Mac

CVE-2023-36895 Outlook

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Office LTSC 2021
Office 2016
Office 2013
Office LTSC for Mac 2021
Office 2019
Office 2019 for Mac
365 Apps Enterprise

CVE-2023-36891 SharePoint Server

Impact, Severity, Disclosure

Spoofing | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

SharePoint Server Subscription Edition
SharePoint Server 2019

Other Products

Exchange Server

CVE-2023-21709 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 9.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

CVE-2023-35368 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 13.

Other Products

Exchange Server

CVE-2023-38185 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 13.

CVE-2023-38182 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 13.

Other Products

Exchange Server

CVE-2023-35388 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 13.

CVE-2023-38181 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

Other Products

Dynamics 365

CVE-2023-35389 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-38167 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Dynamics 365 Business Central 2023 Release Wave 1.

Other Products

SQL Server

CVE-2023-38169 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: ODBC Driver 18 SQL Server on for MacOS, ODBC Driver 17 SQL Server on Linux, SQL Server 2019 (CU 21), ODBC Driver 18 SQL Server on Windows, ODBC Driver 17 SQL Server on Windows, OLE DB Driver 18 SQL Server, OLE DB Driver 19 SQL Server, ODBC Driver 18 SQL Server on Linux, SQL Server 2022 (CU 5), ODBC Driver 17 SQL Server on for MacOS.

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-35390 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, .NET 6.0, .NET 7.0.

CVE-2023-35391 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, .NET 6.0, .NET 7.0.

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-38180 | Important | Denial of Service | Public: No | Exploited: Yes

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, .NET 6.0, .NET 7.0.

Other Products

.NET 6.0

CVE-2023-38178 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, .NET 6.0.

Other Products

.NET Core

CVE-2023-35391 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, .NET 6.0, .NET 7.0.

CVE-2023-38180 | Important | Denial of Service | Public: No | Exploited: Yes

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, .NET 6.0, .NET 7.0.

Other Products

.NET Framework

CVE-2023-36899 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 4.6.2 on Server 2008, .NET Framework 2.0 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 4.8 on Windows 10 1607, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.8 on Server 2008 R2, .NET Framework 4.8 on Server 2012, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2.

Other Products

.NET Framework

CVE-2023-36873 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.4
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.8 on Server 2008 R2, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Server 2022.

Other Products

Visual Studio

CVE-2023-35390 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, .NET 6.0, .NET 7.0.

CVE-2023-35391 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, .NET 6.0, .NET 7.0.

Other Products

Visual Studio

CVE-2023-36897 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Office LTSC 2021, 365 Apps Enterprise, Office 2019, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2010 Tools Office Runtime, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-38178 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, .NET 6.0.

Other Products

Visual Studio

CVE-2023-38180 | Important | Denial of Service | Public: No | Exploited: Yes

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: ASP.NET Core 2.1, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, .NET 6.0, .NET 7.0.

Other Products

Azure DevOps Server

CVE-2023-36869 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Azure DevOps Server 2019.1.2, Azure DevOps Server 2020.1.2, Azure DevOps Server 2022.0.1.

Other Products

Windows Defender Antimalware Platform

CVE-2023-38175 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Windows Defender Antimalware Platm.

Other Products

Azure

CVE-2023-38176 Azure Arc-Enabled Servers

CVE-2023-35393/35394/36877/36881/38188 Azure HDInsights

SA230004 Memory Integrity System Readiness Scan Tool

Summary

The Memory Integrity System Readiness Scan Tool (hvciscan_amd64.exe and hvciscan_arm64.exe) is used to check for compatibility issues with memory integrity, also known as hypervisor-protected code integrity (HVCI). The original version was published without a RSRC section, which contains resource information for a module. The new version addresses this issue. Please see Driver compatibility with memory integrity and VBS for more information.

Recommended Actions:

Install the latest version of the Memory Integrity System Readiness Scan Tool at the download link specified in this advisory.

SA190023 Enabling LDAP Channel Binding and LDAP Signing

What's Changed?

On August 8, 2023, Windows Updates for Server 2022 will add options for administrators to audit client machines that cannot utilize LDAP channel binding tokens via events on Active Directory domain controllers. The updates add the capability to enable CBT events 3074 & 3075 with event source Microsoft-Windows-ActiveDirectory_DomainService in the Directory Service event log.

Recommended Actions:

1. Apply the August 2023 Windows updates
2. Review KB4520412: 2020 LDAP channel binding and LDAP signing requirement for Windows
3. Enable the Auditing Event updates using Group Policy. See steps in KB4520412 for details.

SA230001 Microsoft Signed Drivers Being Used Maliciuosly

What's Changed?

Microsoft is announcing that the August 8, 2023 Window Security updates (see Security Updates table) add additional untrusted drivers and driver signing certificates to the Windows Driver.STL revocation list. Microsoft strongly recommends that customers install the August 2023 updates to add these additional drivers and driver certificates.

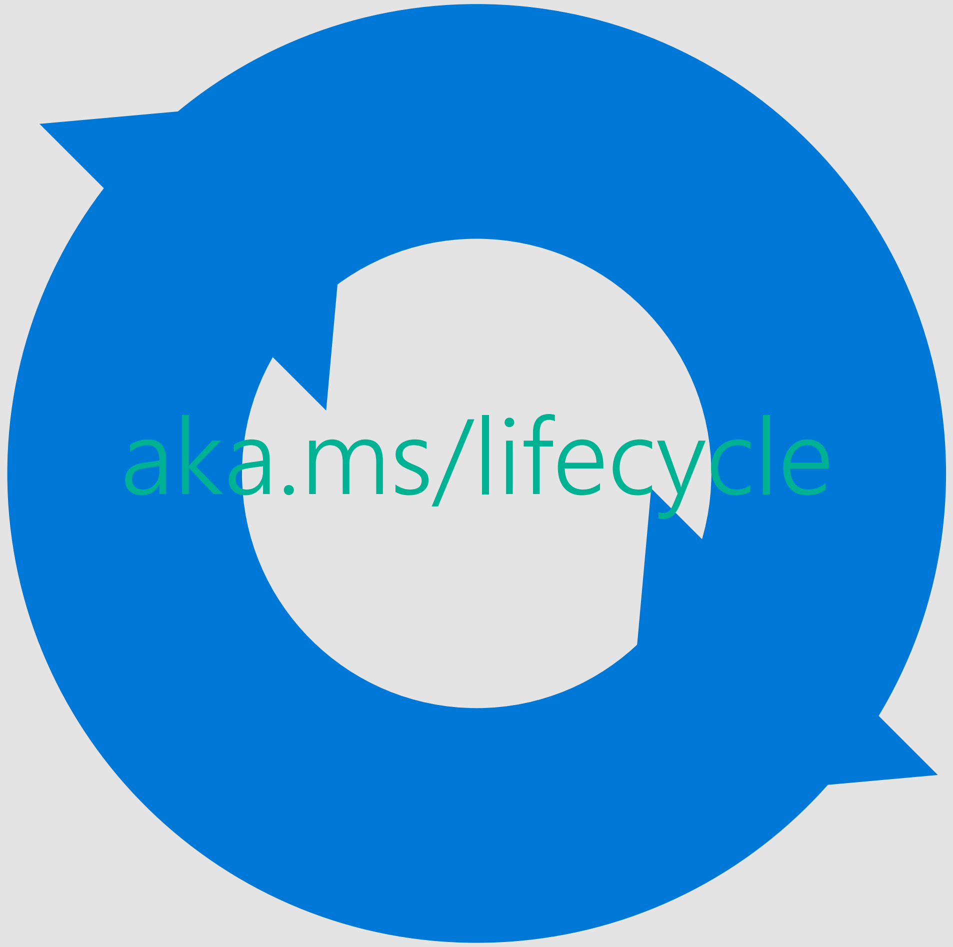
Recommended Actions:

Apply the August 2023 Windows updates.

Product Lifecycle Update

Nothing reaching end of support in August

October 2023 Windows Server 2012 and 2012 R2 will reach end of support



aka.ms/lifecycle

Overview of Windows Server Upgrades

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-35359	No	No	Kernel
CVE-2023-36889	No	No	Group Policy
CVE-2023-36898	No	No	Tablet User Interface Application Core
CVE-2023-36900	No	No	CLFS Driver
CVE-2023-36903	No	No	System Assessment Tool
CVE-2023-36904	No	No	Cloud Files Mini Filter Driver
CVE-2023-36905	No	No	Wireless Wide Area Network Service (WwanSvc)
CVE-2023-36906	No	No	Cryptographic Services
CVE-2023-36907	No	No	Cryptographic Services
CVE-2023-36908	No	No	Hyper-V
CVE-2023-36909	No	No	Message Queuing
CVE-2023-36910	No	No	Message Queuing
CVE-2023-36911	No	No	Message Queuing
CVE-2023-36912	No	No	Message Queuing

CVE	Public	Exploited	Product
CVE-2023-36913	No	No	Message Queuing
CVE-2023-36914	No	No	Smart Card Resource Management Server
CVE-2023-35376	No	No	Message Queuing
CVE-2023-38254	No	No	Message Queuing
CVE-2023-35377	No	No	Message Queuing
CVE-2023-35378	No	No	Projected File System
CVE-2023-35379	No	No	Reliability Analysis Metrics Calculation Engine (RACEng)
CVE-2023-35380	No	No	Kernel
CVE-2023-35381	No	No	Fax Service
CVE-2023-35382	No	No	Kernel
CVE-2023-35383	No	No	Message Queuing
CVE-2023-35384	No	No	HTML Platforms
CVE-2023-35385	No	No	Message Queuing
CVE-2023-35386	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-35387	No	No	Bluetooth A2DP driver
CVE-2023-38186	No	No	Mobile Device Management
CVE-2023-38184	No	No	LDAP
CVE-2023-38175	No	No	Defender
CVE-2023-38172	No	No	Message Queuing
CVE-2023-38170	No	No	HEVC Video Extensions
CVE-2023-20569	No	No	AMD: CVE-2023-20569 Return Address Predictor
CVE-2023-38154	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-38157	No	No	Edge (Chromium-based)
CVE-2023-36865	No	No	Office Visio
CVE-2023-36866	No	No	Office Visio
ADV230003	Yes	Yes	Office Defense in Depth Update
CVE-2023-35371	No	No	Office
CVE-2023-35372	No	No	Office Visio
CVE-2023-36890	No	No	SharePoint Server
CVE-2023-36891	No	No	SharePoint Server
CVE-2023-36892	No	No	SharePoint Server

CVE	Public	Exploited	Product
CVE-2023-36893	No	No	Outlook
CVE-2023-36894	No	No	SharePoint Server
CVE-2023-36895	No	No	Outlook
CVE-2023-36896	No	No	Excel
CVE-2023-36897	No	No	Visual Studio Tools for Office Runtime
CVE-2023-29328	No	No	Teams
CVE-2023-29330	No	No	Teams
CVE-2023-35368	No	No	Exchange
CVE-2023-36869	No	No	Azure DevOps Server
CVE-2023-36873	No	No	.NET Framework
CVE-2023-36876	No	No	Reliability Analysis Metrics Calculation (RacTask)
CVE-2023-36882	No	No	WDAC OLE DB provider for SQL Server
CVE-2023-36899	No	No	ASP.NET

CVE	Public	Exploited	Product
CVE-2023-35389	No	No	Dynamics 365 On-Premises
CVE-2023-35393	No	No	Azure Apache Hive
CVE-2023-35394	No	No	Azure HDInsight Jupyter Notebook
CVE-2023-38188	No	No	Azure Apache Hadoop
CVE-2023-38185	No	No	Exchange Server
CVE-2023-38169	No	No	OLE DB
CVE-2023-38167	No	No	Dynamics Business Central Elevation Of Privilege
CVE-2023-21709	No	No	Exchange Server
CVE-2023-36877	No	No	Azure Apache Oozie
CVE-2023-36881	No	No	Azure Apache Ambari
CVE-2023-35388	No	No	Exchange Server
CVE-2023-35390	No	No	.NET and Visual Studio
CVE-2023-35391	No	No	ASP.NET Core SignalR and Visual Studio
CVE-2023-38182	No	No	Exchange Server

CVE	Public	Exploited	Product
CVE-2023-38181	No	No	Exchange Server
CVE-2023-38180	No	Yes	.NET Core and Visual Studio
CVE-2023-38178	No	No	.NET Core and Visual Studio
CVE-2023-38176	No	No	Azure Arc-Enabled Servers
ADV230004	Yes	No	Memory Integrity System Readiness Scan Tool Defense in Depth Update