Microsoft

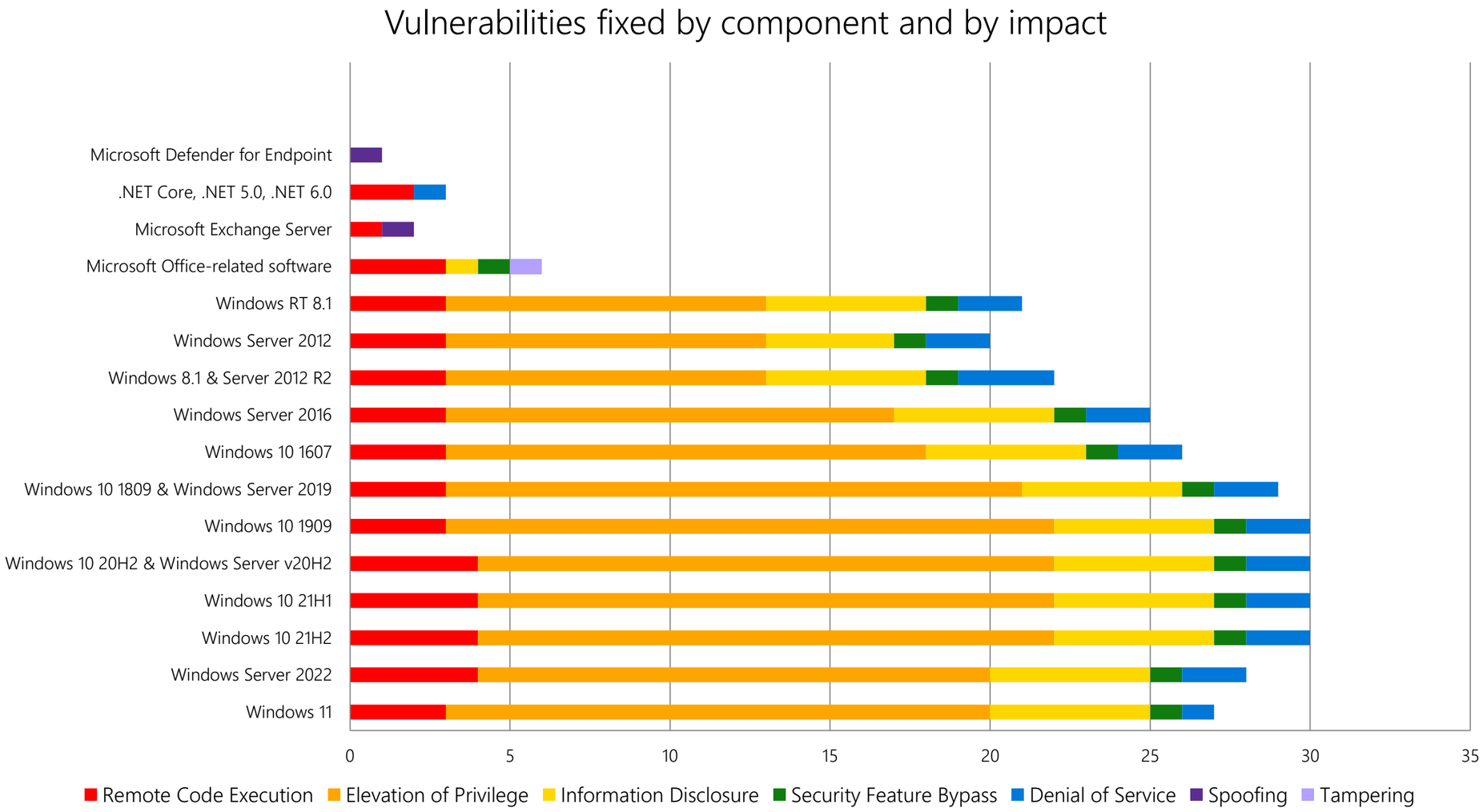
Microsoft Security Release

March 8, 2022

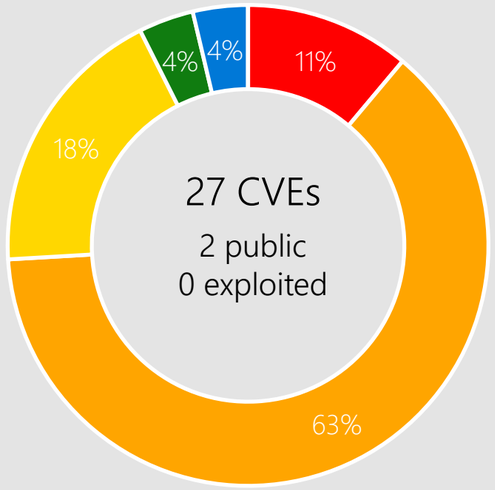
Agenda

- Security Updates
- Product Support Lifecyle
- Other resources related to the release

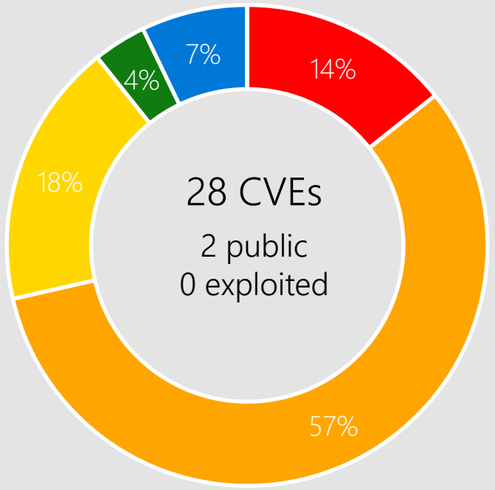
Monthly Security Release Overview - March 2022



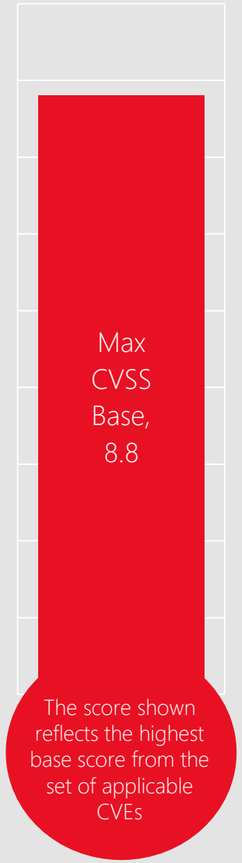
Windows 11, Server 2022



Windows 11



Windows Server 2022



Remote Code Execution | Elevation of Privilege | Information Disclosure | Security Feature Bypass | Denial of Service | Spoofing | Tampering

Affected Components:

ALPC
AFD for WinSock
Cloud Files Mini Filter Driver
CLFS Driver
DWM Core Library
Event Tracing
Fast FAT FS Driver
Fax and Scan Service
HTML Platforms
Hyper-V
Inking COM
Installer
Media Foundation
NTLM
Datagram Receiver Driver
NT OS Kernel
PDEV
PPTP
Print Spooler
Remote Desktop Client
RDP Client
Security Support Provider Interface

CVE-2022-24508 SMBv3 Client/Server

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: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Disable SMBv3 compression. See details in CVE entry.
NOTE: does not prevent exploitation of SMB clients – only SMB servers

Affected Software

Windows 11
Server 2022
Server, version 20H2
Windows 10

CVE-2022-21990 Remote Desktop Client

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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.

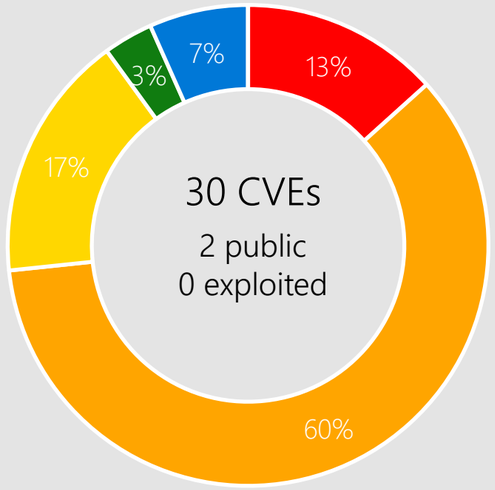
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

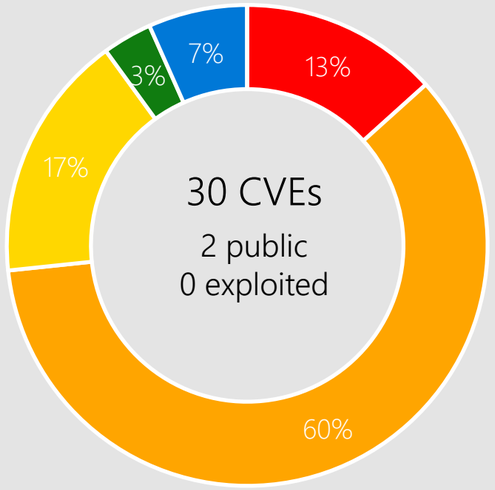
Affected Software

- Windows 11
- Server 2022
- Server, version 20H2
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

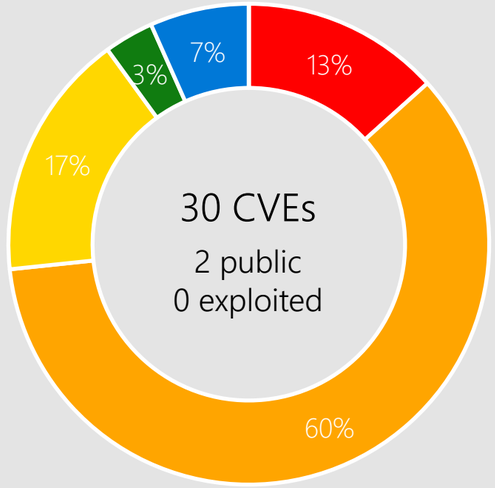
Windows 10



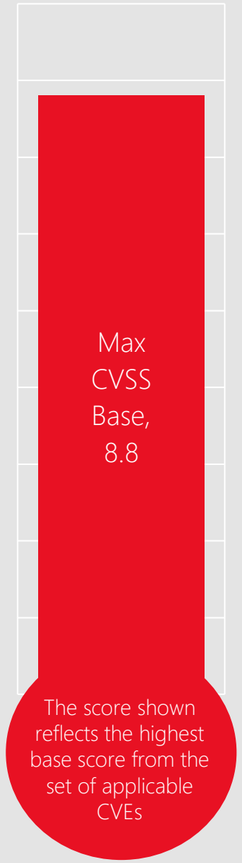
Windows 10 21H2



Windows 10 21H1



Windows 10 20H2 & Windows Server v20H2



Remote Code Execution Elevation of Privilege Information Disclosure Security Feature Bypass Denial of Service Spoofing Tampering

Affected Components:

ALPC
AFD for Winsock
CD-ROM Driver
Cloud Files Mini Filter Driver
CLFS Driver
DWM Core Library
Event Tracing
Fast FAT FS Driver
Fax and Scan Service
HTML Platforms
Hyper-V
Inking COM
Installer
Media Foundation
NTLM
Datagram Receiver Driver
NT OS Kernel
PDEV
PPTP
Print Spooler
Update Stack
Remote Desktop Client
RDP Client
Security Support Provider Interface
Tablet User Interface Application

CVE-2022-23294 Event Tracing

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: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

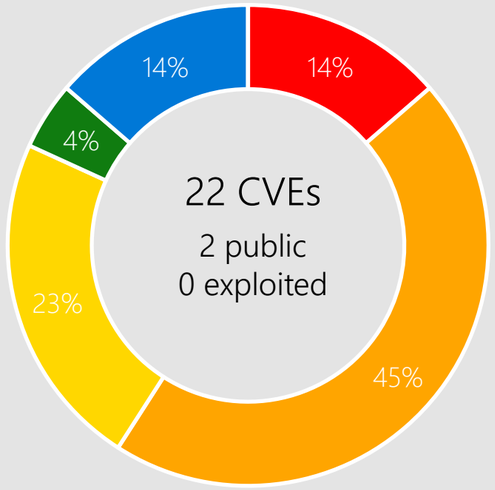
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

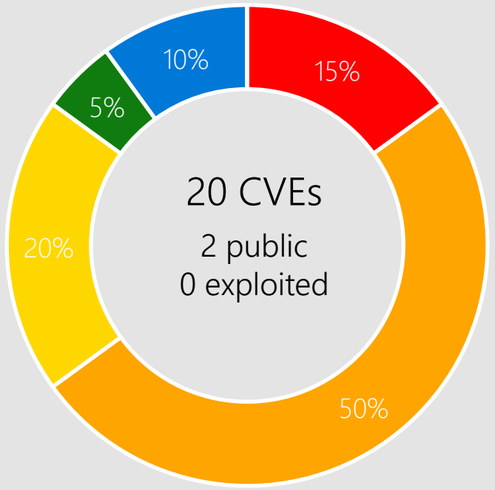
Affected Software

- Windows 11
- Server 2022
- Server, version 20H2
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

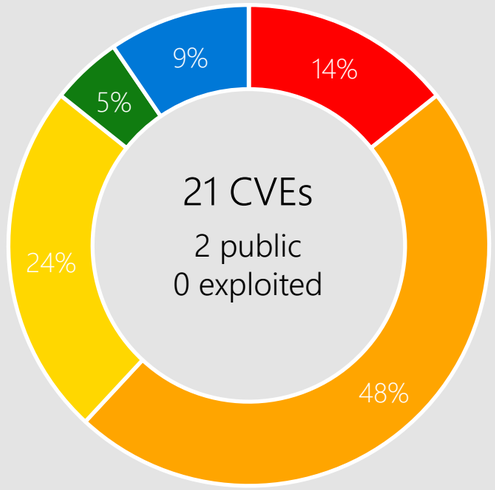
Windows 8.1, Server 2012 R2, and Server 2012



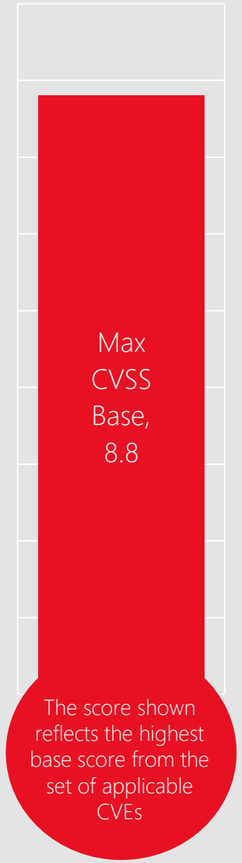
Windows 8.1 & Server 2012 R2



Windows Server 2012



Windows RT 8.1



Remote Code Execution Elevation of Privilege Information Disclosure Security Feature Bypass Denial of Service Spoofing Tampering

Affected Components:

ALPC
CD-ROM Driver
Common Log File System Driver
Event Tracing
Fast FAT File System Driver
Fax and Scan Service
HTML Platforms
Hyper-V
Inking COM
Installer
Media Center Update
Media Foundation
NT Lan Manager Datagram Receiver Driver
NT OS Kernel
PDEV
Point-to-Point Tunneling Protocol
Print Spooler
Remote Desktop Client

CVE-2022-24459 Fax and Scan Service

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly Disclosed | No known exploits in the wild

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

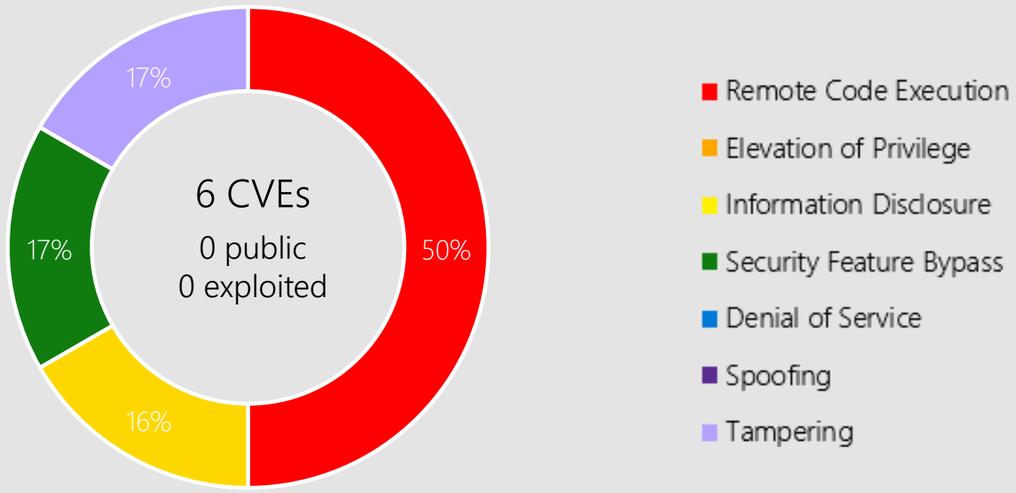
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11
- Server 2022
- Server, version 20H2
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
Word 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Skype Extension Chrome

CVE-2022-24509 Office Visio

Impact, Severity, Disclosure

Remote Code Execution | Important | 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
365 Apps Enterprise
Office 2019

Other Products

Exchange Server

CVE-2022-23277 | Critical | 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 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10.

CVE-2022-24463 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10.

Other Products

Visual Studio

CVE-2020-8927 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), .NET 5.0, .NET 6.0.

CVE-2022-24464 | 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: .NET Core 3.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), .NET 5.0, .NET 6.0.

Other Products

Visual Studio

CVE-2022-24512 | Important | Remote Code Execution | Public: Yes | Exploited: No

CVSS Base Score 6.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Core 3.1, Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), .NET 5.0, .NET 6.0.

CVE-2022-24526 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio Code.

Other Products

.NET Core, .NET 5.0 & .NET 6.0

CVE-2020-8927 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), .NET 5.0, .NET 6.0.

CVE-2022-24464 | 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: .NET Core 3.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), .NET 5.0, .NET 6.0.

Other Products

.NET Core, .NET 5.0 & .NET 6.0

CVE-2022-24512 | Important | Remote Code Execution | Public: Yes | Exploited: No

CVSS Base Score 6.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Core 3.1, Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), .NET 5.0, .NET 6.0.

Other Products

Microsoft Defender for Endpoint

CVE-2022-23278 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.9
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Defender Endpoint Windows on Windows 10, Defender Endpoint Windows on Windows 10 1809, Defender Endpoint Windows on Windows 10 1607, Defender Endpoint Windows on Windows 10 21H1, Defender Endpoint Windows on Windows 10 1909, Defender Endpoint Windows on Windows 10 20H2, Defender Endpoint Windows on Windows 10 21H2, Defender Endpoint Windows on Server, version 20H2, Defender Endpoint Linux, Defender Endpoint for Mac, Defender Endpoint Android, Defender Endpoint Windows on Windows 11, Defender Endpoint Windows on Server 2022 Azure Edition Core Hotpatch, Defender Endpoint Windows on Server 2022, Defender Endpoint Windows on Server 2016, Defender Endpoint Windows on Server 2019.

More Information: https://aka.ms/CVE-2022-23278Post

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-24467/24468/24470/24471/24517/24520 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

CVE-2022-24469 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-24506/24515/24518/24519 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

Other Products

Defender IoT, Mobile

CVE-2022-23282 Paint 3D
CVE-2022-24465 Intune Company Portal for iOS
CVE-2022-23265/CVE-2022-23266 Defender IoT

Product Lifecycle Update

No Products Reaching End-of-Support in March

Windows 10 Semi-Annual Channel end of service May 2022

Windows 10 v1909

Windows 10 20H2 Home and Pro

[Helping customers shift to a modern desktop]

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5001403	April 2021
Windows Server 2012	5011571	March 2022
Windows 10 1607/Server 2016	5011570	March 2022
Windows 10 1809/Server 2019	5005112	August 2021
Windows 10 1909	5005412	August 2021
Windows 10 2004/Windows Server, version 2004	5005260	August 2021
Windows 10 20H2/Windows Server, version 20H2	5005260	August 2021
Windows 10 21H1	5005260	August 2021

4. Why have the 2004, 20H2, and 21H1 rows been added back to the table for the August 2021 updates?
For Windows Server Update Services (WSUS) deployment or when installing the standalone package from Microsoft Update Catalog:
If your devices do not have the May 11, 2021 update (KB5003173) or later LCU, you **must** install the special standalone August 10, 2021 SSU (KB5005260).

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-21977	No	No	Media Foundation
CVE-2022-21967	No	No	Xbox Live Auth Manager for
CVE-2022-22010	No	No	Media Foundation
CVE-2022-21975	No	No	Hyper-V
CVE-2022-21990	Yes	No	Remote Desktop Client
CVE-2022-23290	No	No	Inking COM
CVE-2022-23291	No	No	DWM Core Library
CVE-2022-23293	No	No	Fast FAT File System Driver
CVE-2022-23294	No	No	Event Tracing
CVE-2022-23295	No	No	Raw Image Extension
CVE-2022-23296	No	No	Installer
CVE-2022-23298	No	No	NT OS Kernel
CVE-2022-23299	No	No	PDEV
CVE-2022-23300	No	No	Raw Image Extension

CVE	Public	Exploited	Product
CVE-2022-23301	No	No	HEVC Video Extensions
CVE-2022-22006	No	No	HEVC Video Extensions
CVE-2022-22007	No	No	HEVC Video Extensions
CVE-2022-24451	No	No	VP9 Video Extensions
CVE-2022-24452	No	No	HEVC Video Extensions
CVE-2022-24453	No	No	HEVC Video Extensions
CVE-2022-24501	No	No	VP9 Video Extensions
CVE-2022-24502	No	No	HTML Platforms
CVE-2022-24454	No	No	Security Support Provider Interface
CVE-2022-24503	No	No	Remote Desktop Protocol Client
CVE-2022-24455	No	No	CD-ROM Driver
CVE-2022-24456	No	No	HEVC Video Extensions
CVE-2022-24457	No	No	HEIF Image Extensions
CVE-2022-24507	No	No	Ancillary Function Driver for WinSock

CVE	Public	Exploited	Product
CVE-2022-24459	Yes	No	Fax and Scan Service
CVE-2022-21973	No	No	Media Center Update
CVE-2022-23253	No	No	Point-to-Point Tunneling Protocol
CVE-2022-23281	No	No	Common Log File System Driver
CVE-2022-23283	No	No	ALPC
CVE-2022-23284	No	No	Print Spooler
CVE-2022-23285	No	No	Remote Desktop Client
CVE-2022-23286	No	No	Cloud Files Mini Filter Driver
CVE-2022-23287	No	No	ALPC
CVE-2022-23288	No	No	DWM Core Library
CVE-2022-23297	No	No	NT Lan Manager Datagram Receiver Driver
CVE-2022-24505	No	No	ALPC
CVE-2022-24508	No	No	SMBv3 Client/Server
CVE-2022-24460	No	No	Tablet User Interface Application

CVE	Public	Exploited	Product
CVE-2022-24525	No	No	Update Stack
CVE-2022-24522	No	No	Skype Extension for Chrome
CVE-2022-24509	No	No	Office Visio
CVE-2022-24461	No	No	Office Visio
CVE-2022-24510	No	No	Office Visio
CVE-2022-24462	No	No	Word
CVE-2022-24511	No	No	Office Word
CVE-2022-23265	No	No	Defender for IoT
CVE-2022-23266	No	No	Defender for IoT
CVE-2022-24506	No	No	Azure Site Recovery
CVE-2022-24463	No	No	Exchange Server
CVE-2022-24512	Yes	No	.NET and Visual Studio
CVE-2022-24464	No	No	.NET and Visual Studio
CVE-2022-24465	No	No	Intune Portal for iOS

CVE	Public	Exploited	Product
CVE-2022-24515	No	No	Azure Site Recovery
CVE-2022-24467	No	No	Azure Site Recovery
CVE-2022-23277	No	No	Exchange Server
CVE-2022-23278	No	No	Defender for Endpoint
CVE-2022-23282	No	No	Paint 3D
CVE-2022-24468	No	No	Azure Site Recovery
CVE-2022-24469	No	No	Azure Site Recovery
CVE-2022-24517	No	No	Azure Site Recovery
CVE-2022-24470	No	No	Azure Site Recovery
CVE-2022-24518	No	No	Azure Site Recovery
CVE-2022-24519	No	No	Azure Site Recovery
CVE-2022-24471	No	No	Azure Site Recovery
CVE-2022-24520	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2020-8927	No	No	Brotli Library Buffer Overflow
CVE-2022-24526	No	No	Visual Studio Code