Microsoft

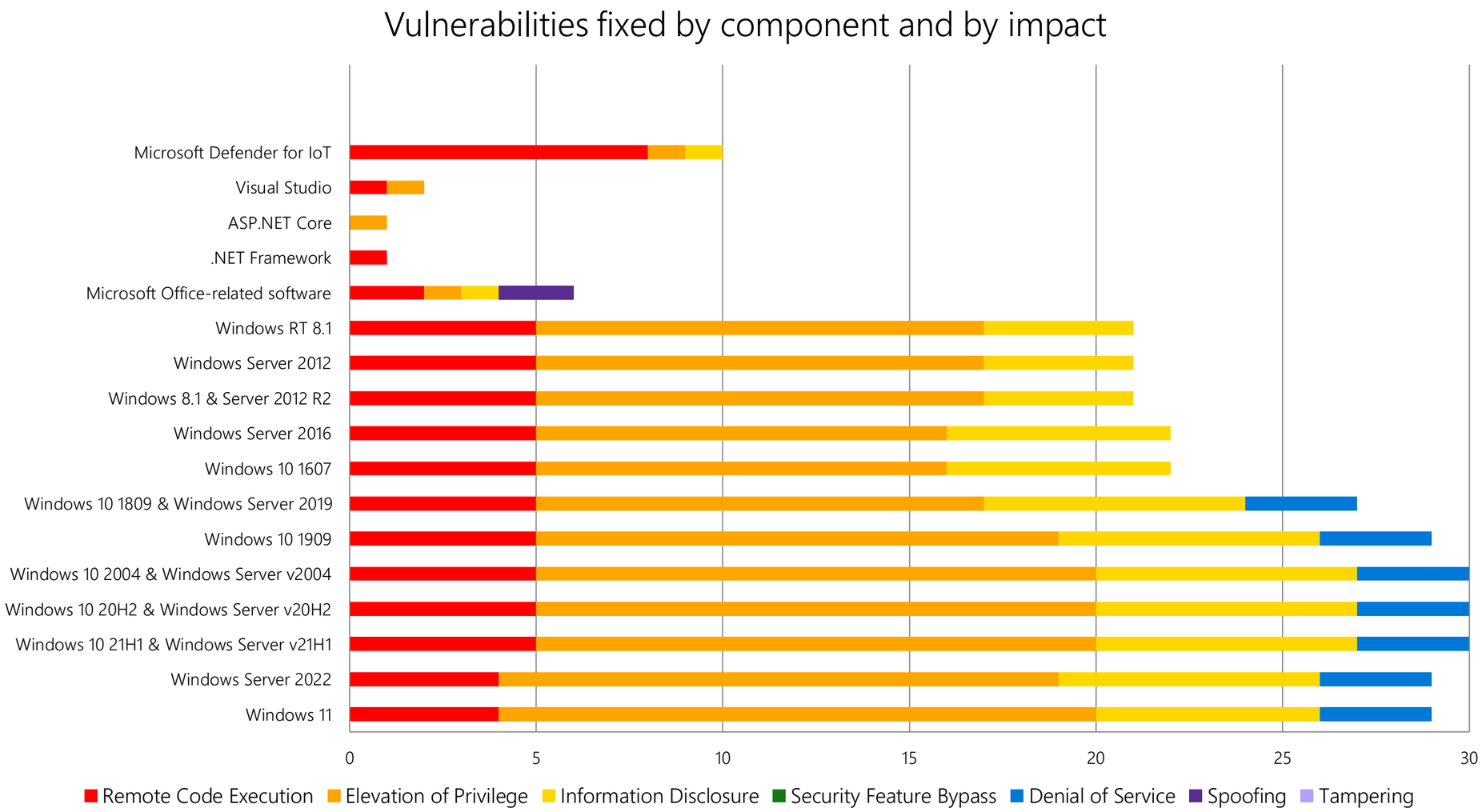
Microsoft Security Release

December 14, 2021

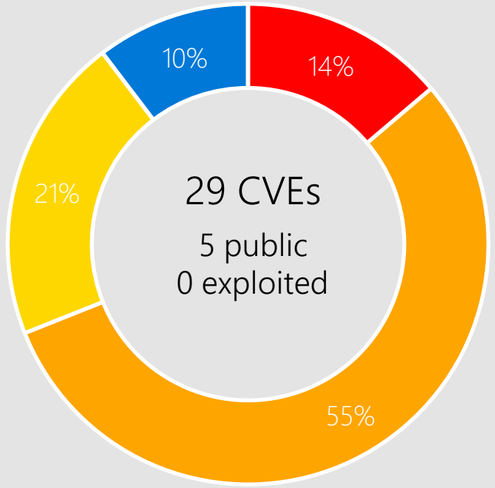
Agenda

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

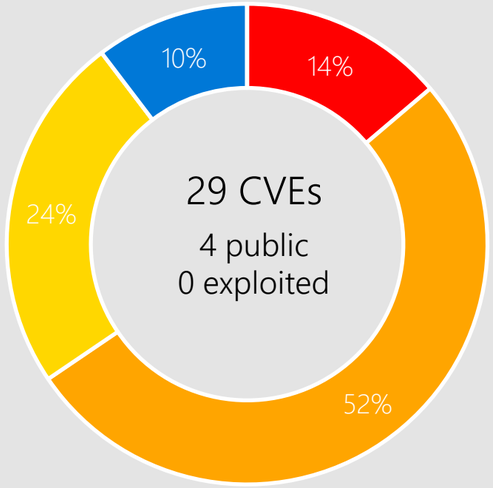
Monthly Security Release Overview - December 2021



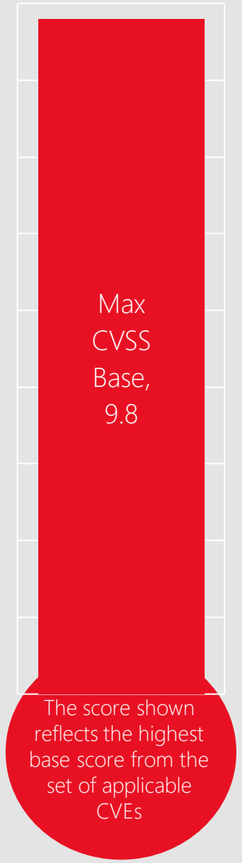
Windows 11, Server 2022



Windows 11



Windows Server 2022



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

Affected Components:

Common Log File
System Driver
Digital Media Receiver
DirectX
EFS

Event Tracing
Fax Service
Hyper-V
Windows Installer

Kernel
LSA Server
Message Queuing
NTFS
SymCrypt

Print Spooler
Recovery Environment Agent
Remote Access

RA Connection Manager
Remote Desktop Client
Setup
Storage Spaces Controller

CVE-2021-43215 iSNS

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

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, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-43880 Mobile Device Management

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 5.5 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

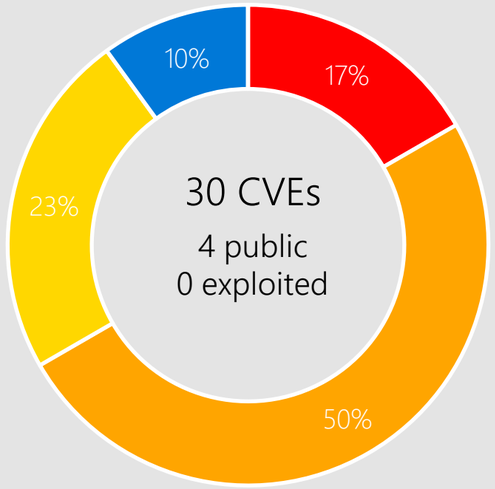
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

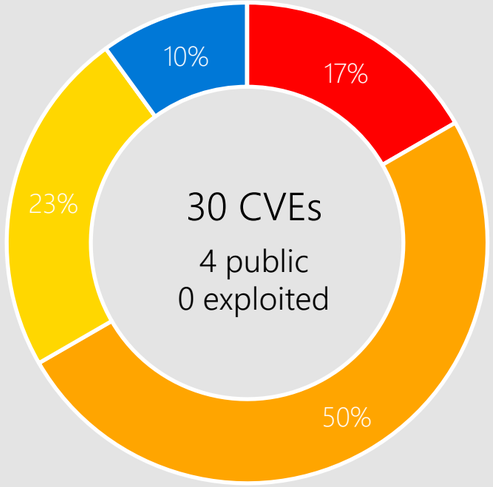
Affected Software

Windows 11

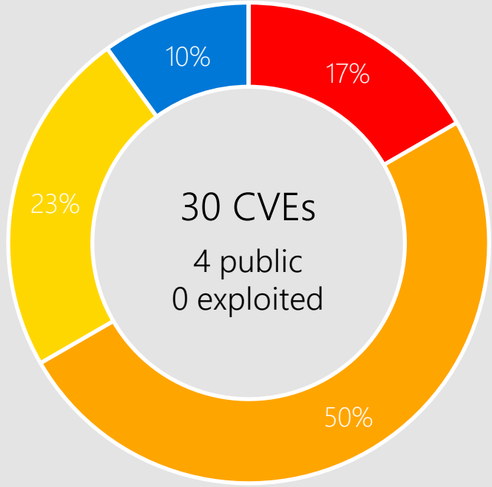
Windows 10



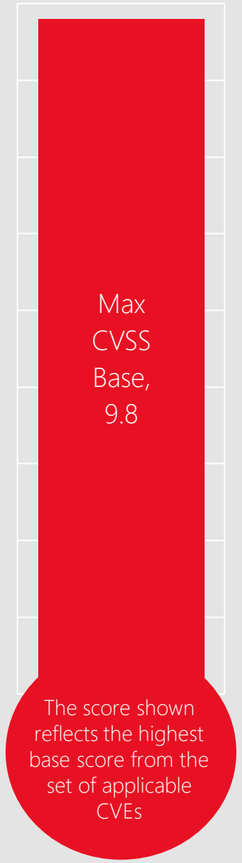
Windows 10 21H1



Windows 10 20H2 & Windows Server v20H2



Windows 10 2004 & Windows Server v2004



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

Affected Components:

Common Log File System Driver
Digital Media Receiver
DirectX
Event Tracing
Fax Service
Hyper-V
Windows Installer
iSNS Server
Kernel
LSA Server
Message Queuing
NTFS
Print Spooler
Recovery Environment Agent
Remote Access
RA Connection Manager
Remote Desktop Client Setup
Storage Spaces Controller
EFS

CVE-2021-43217 Encrypting File System (EFS)

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.1 | Attack Vector: Network | Attack Complexity: High | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

More Information

EFS security hardening changes in CVE-2021-43217
https://support.microsoft.com/help/5009763

Affected Software

Windows 11
Server 2022
Server, version 20H2
Server, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-43233 Remote Desktop Client

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Network | Attack Complexity: High | 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, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-43240 NTFS Set Short Name

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.

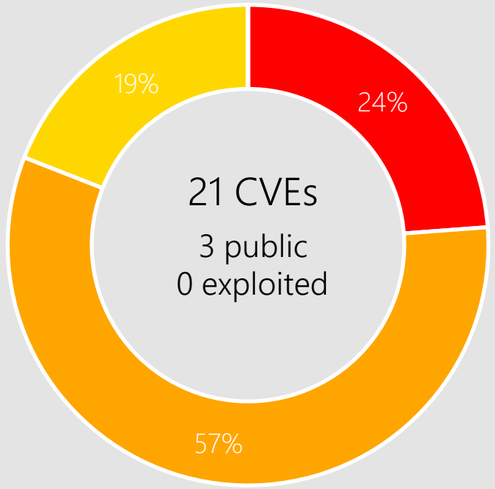
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

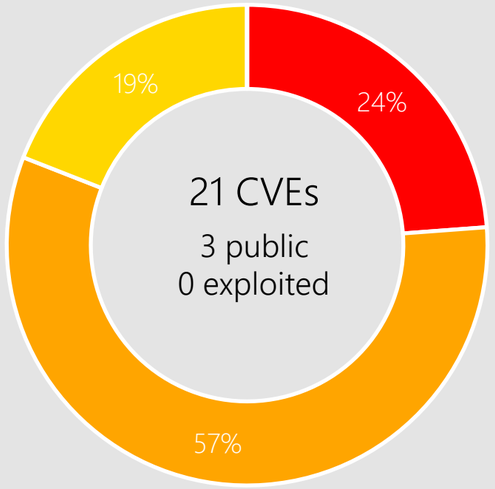
Affected Software

Windows 11
Server 2022
Server, version 20H2
Server, version 2004
Windows 10

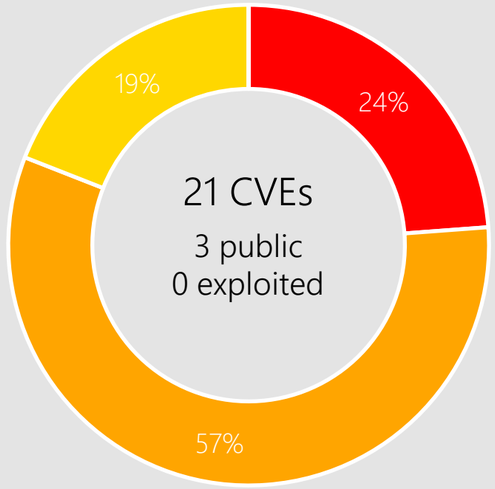
Windows 8.1, Server 2012 R2, and Server 2012



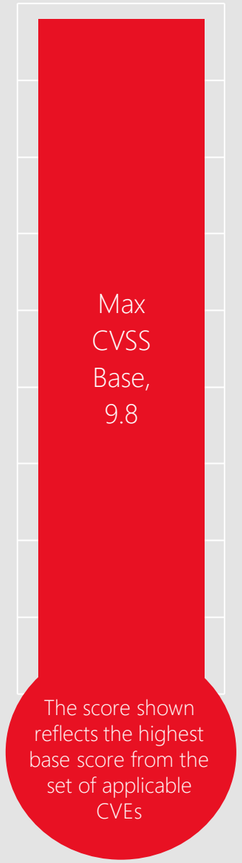
Windows 8.1 & Server 2012 R2



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:

Common Log File System Driver
Digital Media Receiver
Digital TV Tuner
Encrypting File System (EFS)
Event Tracing
Fax Service
Windows Installer
iSNS Server
LSA Server
Media Center
Message Queuing
NTFS
Print Spooler
Remote Access
RA Connection Manager

CVE-2021-41333 Print Spooler

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, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-43883 Installer

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.

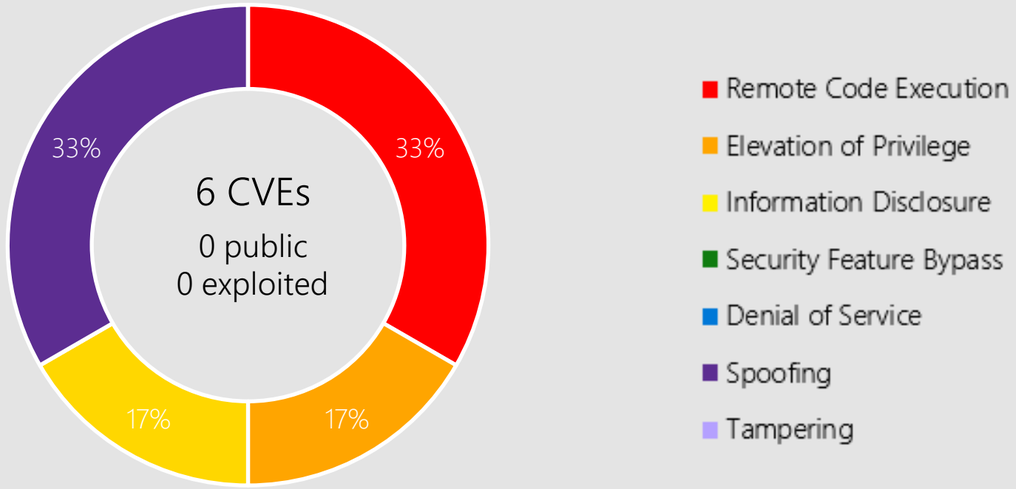
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11
- Server 2022
- Server, version 20H2
- Server, version 2004
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Server Subscription Edition Language Pack

CVE-2021-42309 SharePoint 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

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

SharePoint Server Subscription Edition
SharePoint Foundation 2013
SharePoint Enterprise Server 2016
SharePoint Server 2019

CVE-2021-43256 Excel

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

Excel 2016
Excel 2013
Office Web Apps Server 2013
Office Online Server
365 Apps Enterprise
Office LTSC 2021

Other Products

.NET Core

CVE-2021-43877 | 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: ASP.NET Core 5.0, ASP.NET Core 3.1, ASP.NET Core 6.0, 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), Visual Studio 2022 version 17.0.

Other Products

Visual Studio

CVE-2021-43877 | 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: ASP.NET Core 5.0, ASP.NET Core 3.1, ASP.NET Core 6.0, 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), Visual Studio 2022 version 17.0.

Other Products

PowerShell

CVE-2021-43896 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: PowerShell 7.2.

Other Products

Microsoft 4K Wireless Display Adapter

CVE-2021-43899 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: 4K Wireless Display Adapter.

Other Products

Developer tools, Defender IoT and Mobile

CVE-2021-43905 Office App CVSS score: 9.6
CVE-2021-43907 VS Code WSL Extension CVSS score: 9.8
CVE-2021-43890 Windows AppX Installer
CVE-2021-43225 Bot Framework SDK for .NET Framework
CVE-2021-43891/43908 VS Code
CVE-2021-43892 BizTalk ESB Toolkit
CVE-2021-41365/42310/42311/42312/42313/42314/42315/43882/43888/43889 Defender IoT

Product Lifecycle Update

No fixed lifecycle products reaching end of support in December

Windows 10 Semi-Annual Channel end of service
Windows 10 2004 - December
Server version 2004 - December

Helping customers shift to a modern desktop

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2021-40441	No	No	Media Center
CVE-2021-40452	No	No	HEVC Video Extensions
CVE-2021-40453	No	No	HEVC Video Extensions
CVE-2021-43214	No	No	Web Media Extensions
CVE-2021-43217	No	No	Encrypting File System (EFS)
CVE-2021-43219	No	No	DirectX Graphics Kernel File
CVE-2021-43223	No	No	Remote Access Connection Manager
CVE-2021-43224	No	No	CLFS Driver
CVE-2021-43226	No	No	CLFS Driver
CVE-2021-43227	No	No	Storage Spaces Controller
CVE-2021-43228	No	No	SymCrypt
CVE-2021-43229	No	No	NTFS
CVE-2021-43230	No	No	NTFS
CVE-2021-43231	No	No	NTFS

CVE	Public	Exploited	Product
CVE-2021-43232	No	No	Event Tracing
CVE-2021-43234	No	No	Fax Service
CVE-2021-43235	No	No	Storage Spaces Controller
CVE-2021-43237	No	No	Setup
CVE-2021-43238	No	No	Remote Access
CVE-2021-43239	No	No	Recovery Environment Agent
CVE-2021-43240	Yes	No	NTFS Set Short Name
CVE-2021-43243	No	No	VP9 Video Extensions
CVE-2021-43244	No	No	Kernel
CVE-2021-43245	No	No	Digital TV Tuner
CVE-2021-43246	No	No	Hyper-V
CVE-2021-43247	No	No	TCP/IP Driver
CVE-2021-43248	No	No	Digital Media Receiver
CVE-2021-43875	No	No	Office Graphics

CVE	Public	Exploited	Product
CVE-2021-41333	Yes	No	Print Spooler
CVE-2021-41360	No	No	HEVC Video Extensions
CVE-2021-43207	No	No	Common Log File System Driver
CVE-2021-43880	Yes	No	Mobile Device Management
CVE-2021-43883	Yes	No	Installer
CVE-2021-43893	Yes	No	Encrypting File System (EFS)

CVE	Public	Exploited	Product
CVE-2021-43255	No	No	Office Trust Center
CVE-2021-43256	No	No	Excel
CVE-2021-42293	No	No	Jet Red Database Engine and Access Connectivity Engine
CVE-2021-42294	No	No	SharePoint Server
CVE-2021-42295	No	No	Visual Basic for Applications
CVE-2021-42309	No	No	SharePoint Server

CVE	Public	Exploited	Product
CVE-2021-42320	No	No	SharePoint Server
CVE-2021-43242	No	No	SharePoint Server
CVE-2021-43905	No	No	Office app
CVE-2021-42310	No	No	Defender for IoT
CVE-2021-42311	No	No	Defender for IoT
CVE-2021-42312	No	No	Defender for IOT
CVE-2021-42313	No	No	Defender for IoT
CVE-2021-42314	No	No	Defender for IoT
CVE-2021-42315	No	No	Defender for IoT
CVE-2021-43215	No	No	iSNS Server Can Lead to
CVE-2021-43216	No	No	Local Security Authority Server (lsasrv)
CVE-2021-43222	No	No	Message Queuing
CVE-2021-43225	No	No	Bot Framework SDK
CVE-2021-43233	No	No	Remote Desktop Client

CVE	Public	Exploited	Product
CVE-2021-43236	No	No	Message Queuing
CVE-2021-43877	No	No	ASP.NET Core and Visual Studio
CVE-2021-43882	No	No	Defender for IoT
CVE-2021-43888	No	No	Defender for IoT
CVE-2021-43889	No	No	Defender for IoT
CVE-2021-43891	No	No	Visual Studio Code
CVE-2021-43899	No	No	4K Wireless Display Adapter
CVE-2021-43907	No	No	Visual Studio Code WSL Extension
CVE-2021-41365	No	No	Defender for IoT
CVE-2021-43896	No	No	PowerShell