Microsoft

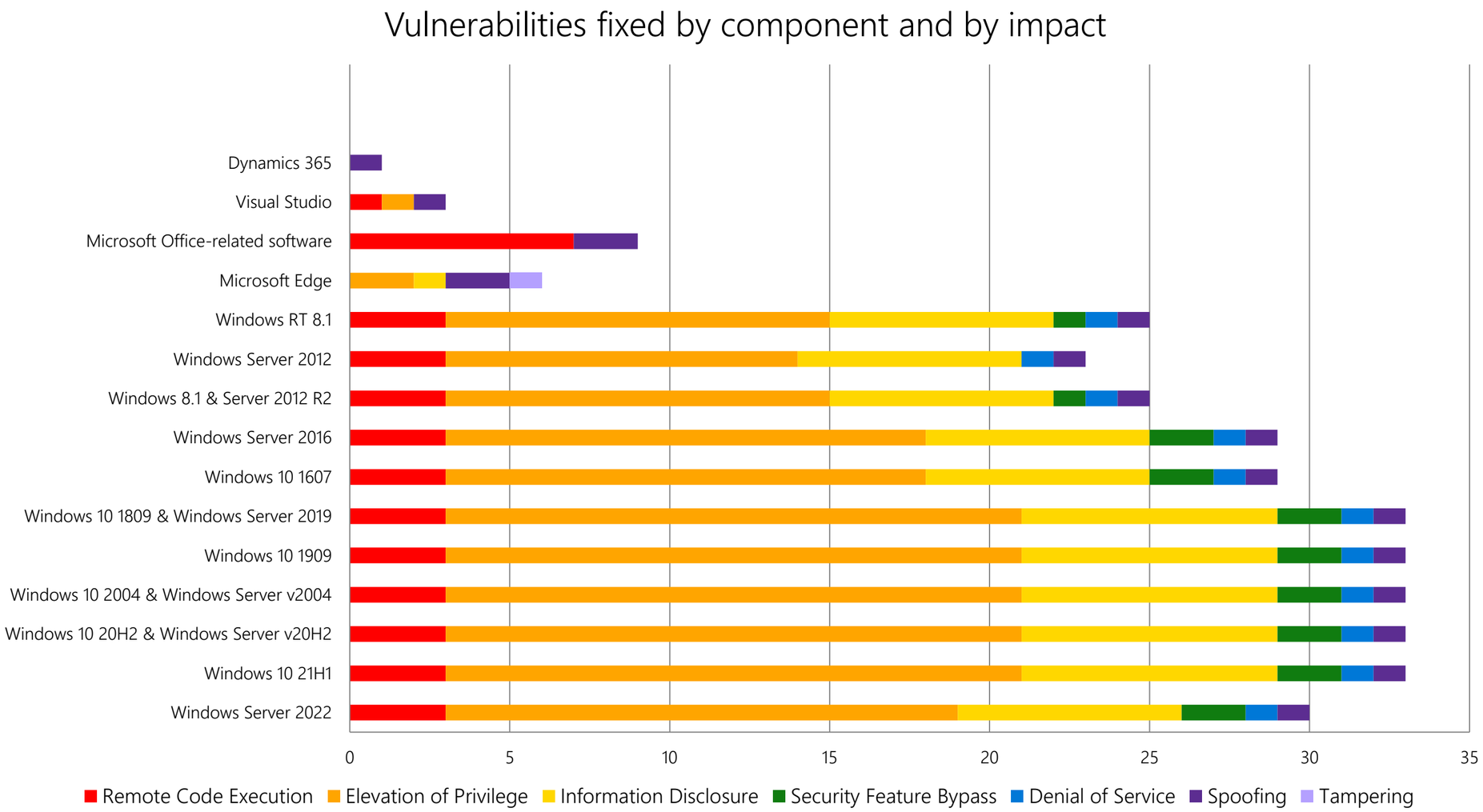
Microsoft Security Release

September 14, 2021

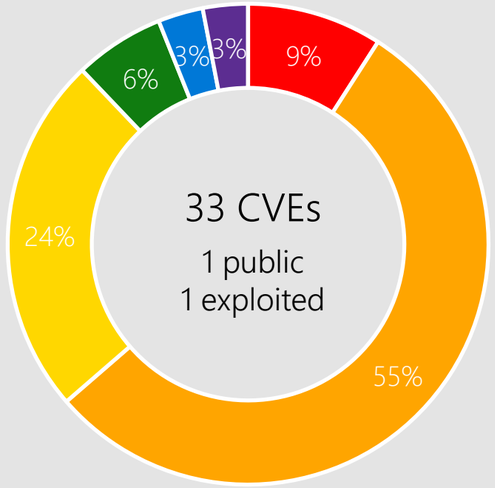
Agenda

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

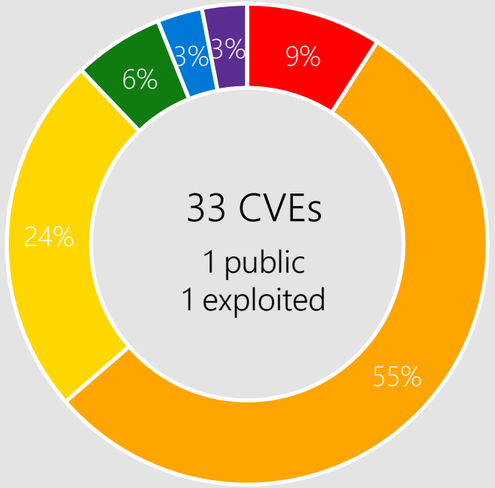
Monthly Security Release Overview - September 2021



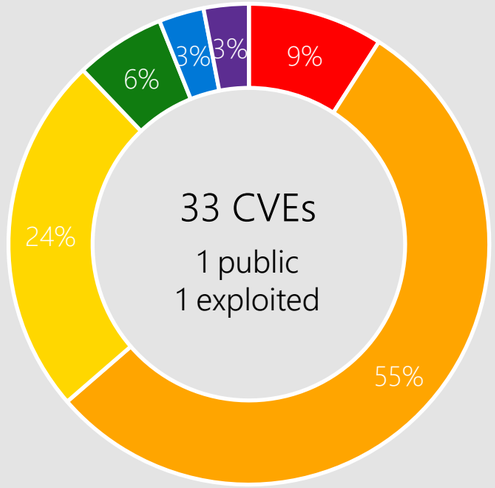
Windows 10



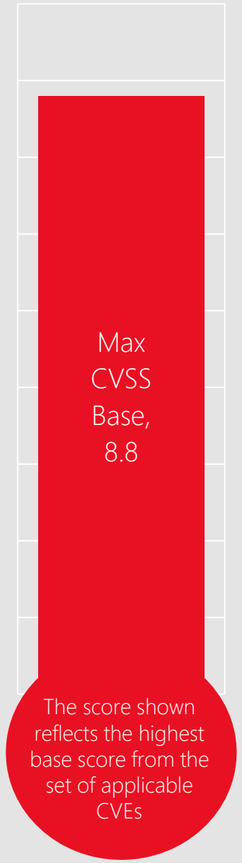
Windows 10 21H1 & Windows Server v21H1



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:

Ancillary Function Driver for WinSock
Authenticode
Bind Filter Driver
BitLocker
Common Log File System Driver
Event Tracing
Installer
Key Storage Provider
MSHTML
Print Spooler
Redirected Drive Buffering SubSystem Driver
Redirected Drive Buffering System
Scripting Engine
SMB
Storage
Subsystem for Linux
Update Client
Win32k

CVE-2021-40444 MSHTML

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly Disclosed | Exploitation Detected

CVSSScoreMetrics

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

Mitigations

By default, Microsoft Office opens documents from the internet in Protected View or Application Guard for Office both of which prevent the current attack.

Workarounds

Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. See CVE entry for details.

Affected Software

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

CVE-2021-36965 WLAN AutoConfig Service

Impact, Severity, Disclosure

Remote Code Execution | Critical | 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: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

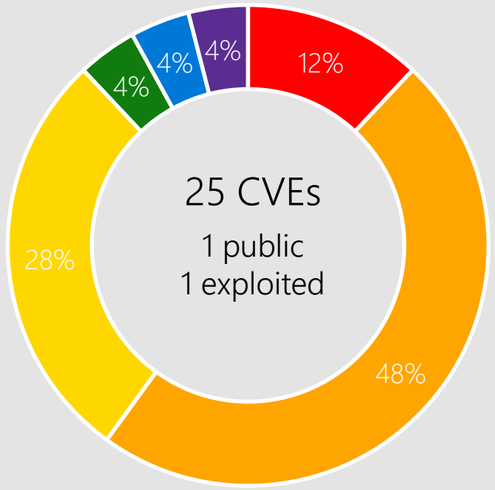
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

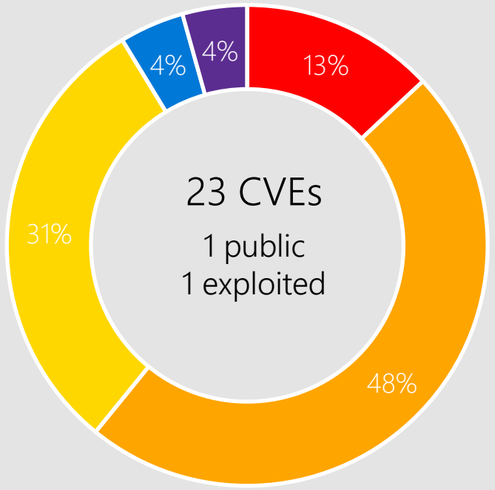
Affected Software

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

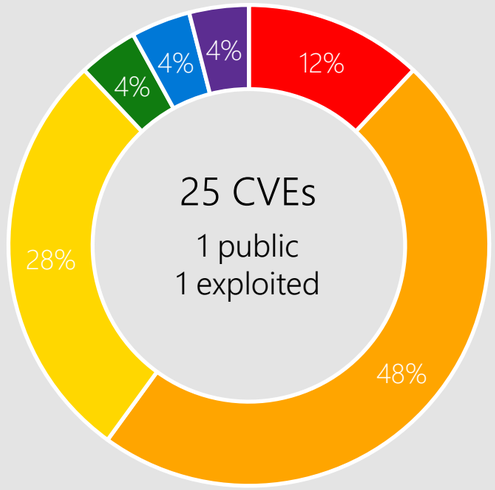
Windows 8.1, Server 2012 R2, and Server 2012



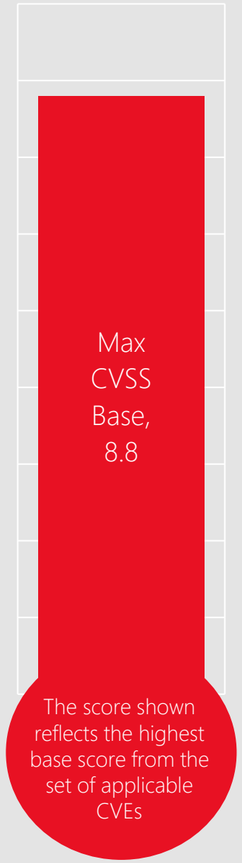
Windows 8.1 & Server 2012 R2



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:

Ancillary Function Driver for WinSock
Authenticode
Common Log File System Driver
Event Tracing
Installer
Key Storage Provider
MSHTML
Print Spooler
Redirected Drive Buffering SubSystem Driver
Scripting Engine
SMB
Win32k

CVE-2021-36958 Print Spooler

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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.

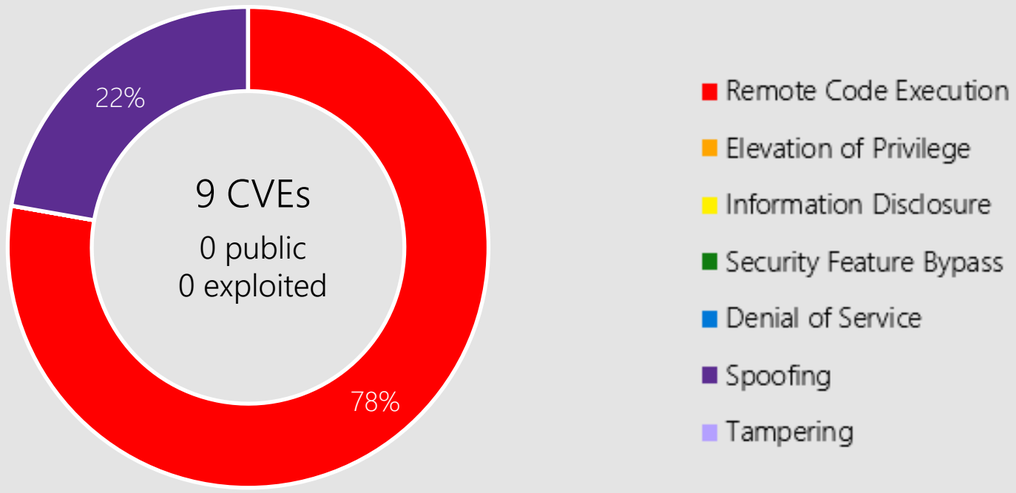
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office 2019 for Mac
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013

CVE-2021-38658 Office Graphics

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 2016
Office 2013
Office 2019
Office 2019 for Mac

CVE-2021-38655 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
365 Apps Enterprise
Office 2019
Office 2019 for Mac
Office Online Server

CVE-2021-38646 Office Access Connectivity Engine

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 2016
Office 2013
Office 2019
365 Apps Enterprise

CVE-2021-38651 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.6 | 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 Foundation 2013
SharePoint Server 2019
SharePoint Enterprise Server 2016

Other Products

Dynamics 365

CVE-2021-40440 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.5, Dynamics 365 Business Central 2020 Release Wave 2 – Update 17.10.

Other Products

Visual Studio

CVE-2021-26434 | 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: Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3).

CVE-2021-26437 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio Code.

Other Products

Visual Studio

CVE-2021-36952 | 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 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8).

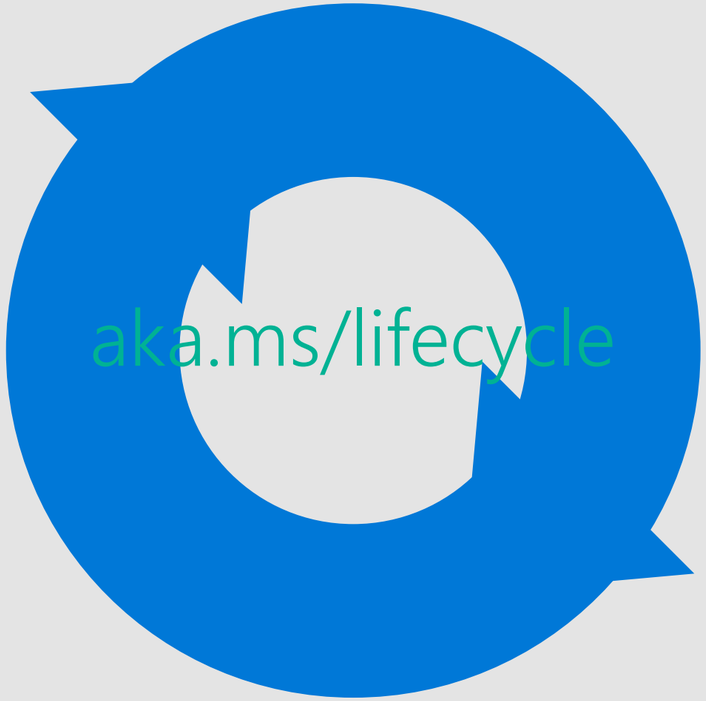
Other Products

Azure and Mobile

CVE-2021-40448 Accessibility Insights for Android
CVE-2021-38645/38647/38648/38649 Azure Open Management Infrastructure
CVE-2021-36956 Azure Sphere

Product Lifecycle Update

Visio Services in SharePoint retires Sep 30, 2021 (originally set to retire Sep 30, 2020)



https://techcommunity.microsoft.com/t5/visio-blog/visio-web-access-aka-visio-services-updates/ba-p/109541

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5001403	April 2021
Windows Server 2012	5001401	April 2021
Windows 10 1607/Server 2016	5005698	September 2021
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-2021-36954	No	No	Bind Filter Driver
CVE-2021-36955	No	No	CLFS Driver
CVE-2021-36959	No	No	Authenticode
CVE-2021-36960	No	No	SMB
CVE-2021-36961	No	No	Installer
CVE-2021-36962	No	No	Installer
CVE-2021-36963	No	No	CLFS Driver
CVE-2021-36964	No	No	Event Tracing
CVE-2021-36965	No	No	WLAN AutoConfig Service
CVE-2021-36966	No	No	Subsystem for Linux
CVE-2021-36967	No	No	WLAN AutoConfig Service
CVE-2021-36968	Yes	No	DNS
CVE-2021-36969	No	No	Redirected Drive Buffering SubSystem Driver
CVE-2021-36972	No	No	SMB

CVE	Public	Exploited	Product
CVE-2021-36973	No	No	Redirected Drive Buffering System
CVE-2021-36974	No	No	SMB
CVE-2021-36975	No	No	Win32k
CVE-2021-26435	No	No	Scripting Engine
CVE-2021-38624	No	No	Key Storage Provider
CVE-2021-38625	No	No	Kernel
CVE-2021-38626	No	No	Kernel
CVE-2021-38628	No	No	AFD for WinSock
CVE-2021-38629	No	No	AFD for WinSock
CVE-2021-38630	No	No	Event Tracing
CVE-2021-38632	No	No	BitLocker
CVE-2021-38633	No	No	CLFS Driver
CVE-2021-38634	No	No	Update Client
CVE-2021-38635	No	No	Redirected Drive Buffering SubSystem Driver

CVE	Public	Exploited	Product
CVE-2021-38636	No	No	Redirected Drive Buffering SubSystem Driver
CVE-2021-38637	No	No	Storage
CVE-2021-38638	No	No	AFD for WinSock
CVE-2021-40444	Yes	Yes	MSHTML
CVE-2021-38639	No	No	Win32k
CVE-2021-38657	No	No	Office Graphics Component
CVE-2021-38658	No	No	Office Graphics
CVE-2021-38660	No	No	Office Graphics
CVE-2021-38661	No	No	HEVC Video Extensions
CVE-2021-38667	No	No	Print Spooler
CVE-2021-38671	No	No	Print Spooler
CVE-2021-40447	No	No	Print Spooler
CVE-2021-26436	No	No	Edge (Chromium-based)
CVE-2021-38641	No	No	Edge for Android

CVE	Public	Exploited	Product
CVE-2021-38642	No	No	Edge for iOS
CVE-2021-38669	No	No	Edge (Chromium-based)
CVE-2021-26439	No	No	Edge for Android
CVE-2021-36930	No	No	Edge (Chromium-based)
CVE-2021-30606	No	No	Chromium
CVE-2021-30607	No	No	Chromium
CVE-2021-30608	No	No	Chromium
CVE-2021-30609	No	No	Chromium
CVE-2021-30610	No	No	Chromium
CVE-2021-30611	No	No	Chromium
CVE-2021-30612	No	No	Chromium
CVE-2021-30613	No	No	Chromium
CVE-2021-30614	No	No	Chromium
CVE-2021-30615	No	No	Chromium

CVE	Public	Exploited	Product
CVE-2021-30616	No	No	Chromium
CVE-2021-30617	No	No	Chromium
CVE-2021-30618	No	No	Chromium
CVE-2021-30619	No	No	Chromium
CVE-2021-30620	No	No	Chromium
CVE-2021-30621	No	No	Chromium
CVE-2021-30622	No	No	Chromium
CVE-2021-30623	No	No	Chromium
CVE-2021-30624	No	No	Chromium
CVE-2021-38646	No	No	Office Access Connectivity Engine
CVE-2021-38650	No	No	Office
CVE-2021-38651	No	No	SharePoint Server
CVE-2021-38652	No	No	SharePoint Server
CVE-2021-38653	No	No	Office Visio

CVE	Public	Exploited	Product
CVE-2021-38654	No	No	Office Visio
CVE-2021-38655	No	No	Excel
CVE-2021-38656	No	No	Word
CVE-2021-38659	No	No	Office
CVE-2021-40448	No	No	Accessibility Insights for Android
CVE-2021-36952	No	No	Visual Studio
CVE-2021-38645	No	No	Open Mgmt Infrastructure
CVE-2021-38647	No	No	Open Mgmt Infrastructure
CVE-2021-38648	No	No	Open Mgmt Infrastructure
CVE-2021-38649	No	No	Open Mgmt Infrastructure
CVE-2021-26437	No	No	Visual Studio Code
CVE-2021-40440	No	No	Dynamics Business Central Cross-site Scripting
CVE-2021-36956	No	No	Azure Sphere
CVE-2021-26434	No	No	Visual Studio

CVE	Public	Exploited	Product
CVE-2021-38644	No	No	MPEG-2 Video Extension