Microsoft

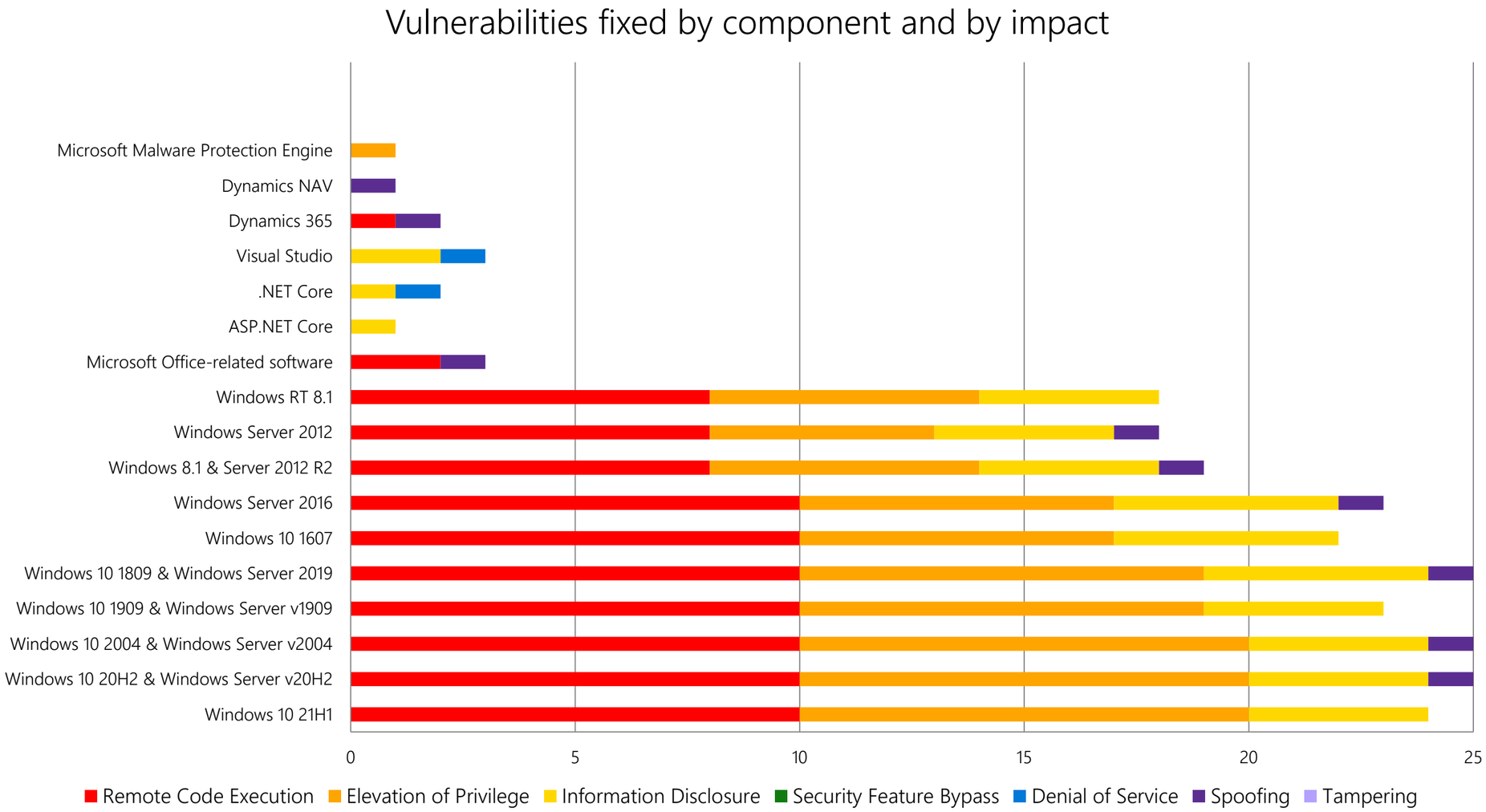
Microsoft Security Release

August 10, 2021

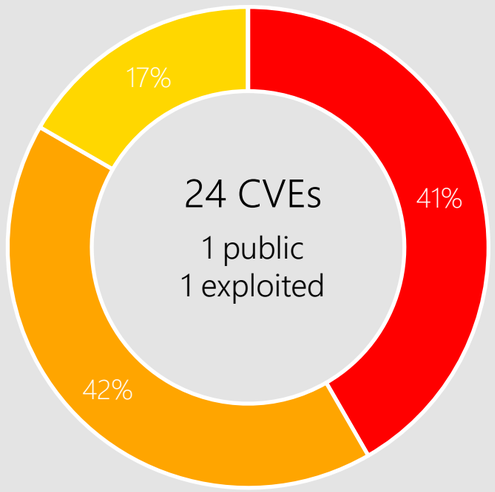
Agenda

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

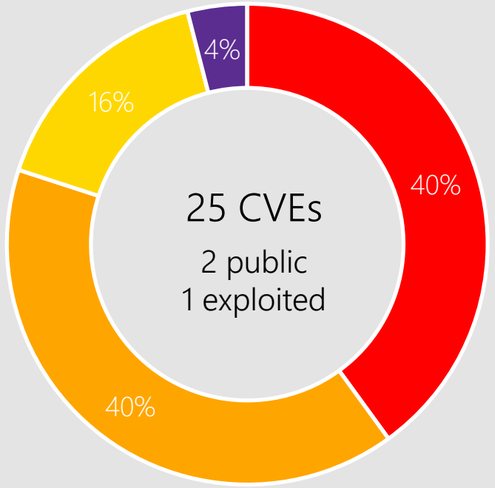
Monthly Security Release Overview - August 2021



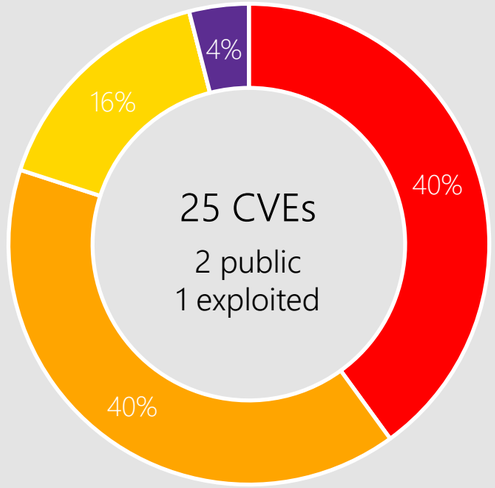
Windows 10



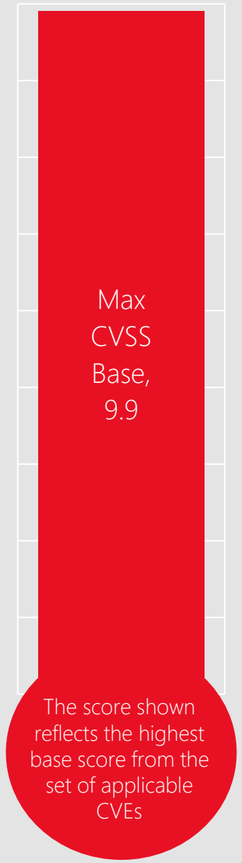
Windows 10 21H1



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:

Bluetooth Driver	Graphics Component	Media MPEG-4 Video Decoder	Remote Desktop Client	Storage Spaces Controller
Cryptographic Primitives Library	Graphics Component	MSHTML Platform	Scripting Engine	TCP/IP
Event Tracing	Font Parsing	Print Spooler	Services for NFS	Update Medic Service
	LSA		ONCRPC XDR Driver	

Print Spooler Vulnerabilities

CVE-2021-36936 Impact, Severity, Disclosure

Remote Code Execution | Critical | Publicly Disclosed | No known exploits in the wild

CVE-2021-36936 CVSSScoreMetrics

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

CVE-2021-36947 Impact, Severity, Disclosure

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

CVE-2021-36947 CVSSScoreMetrics

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

CVE-2021-34483 Impact, Severity, Disclosure

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

CVE-2021-34483 CVSSScoreMetrics

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

Affected Software

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

Print Functionality Changes

What's Changed?

After applying August 2021 updates, default Point and Print driver installation and update will require administrator privileges. The current default behavior (allowing non-administrators to perform these actions) does not provide customers with the level of security required to protect against these attacks. These changes are associated with CVE-2021-34481, initially released July 15, 2021.

Suggested Actions:

1. Apply the August 2021 Windows updates
2. Review KB5005652 for details on managing Point and Print default driver installation behavior
3. If you must revert to less secure print driver installation and update, apply mitigations listed in KB5005652

https://aka.ms/PointPrintMSRCBlog

CVE-2021-26424 TCP/IP

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.9 | 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

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

CVE-2021-36948 Update Medic Service

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

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

Server, version 20H2
Windows 10
Server, version 2004
Server 2019

CVE-2021-36934 Windows

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

Workarounds

1. Restrict access to the contents of %windir%\system32\config
2. Delete Volume Shadow Copy Service (VSS) copies

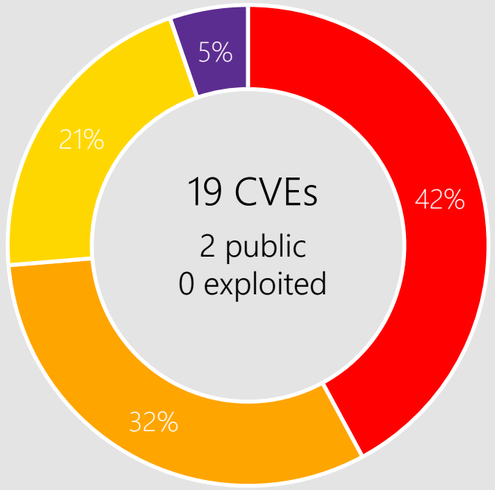
See KB5005357 - Delete Volume Shadow Copies for details

NOTE: after applying the August updates, it is still necessary to delete the VSS copies to completely address the issue. This CVE was initially released July 20; however, a security update is now available.

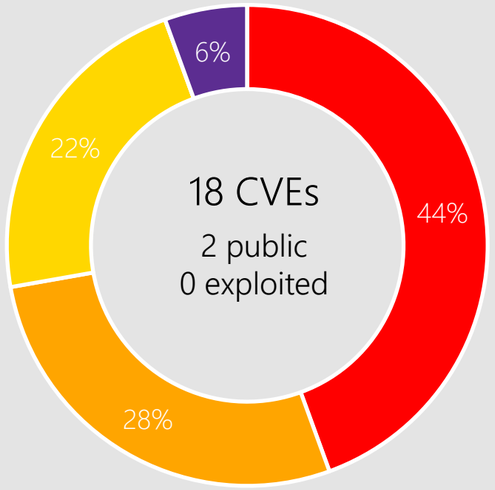
Affected Software

Windows 10

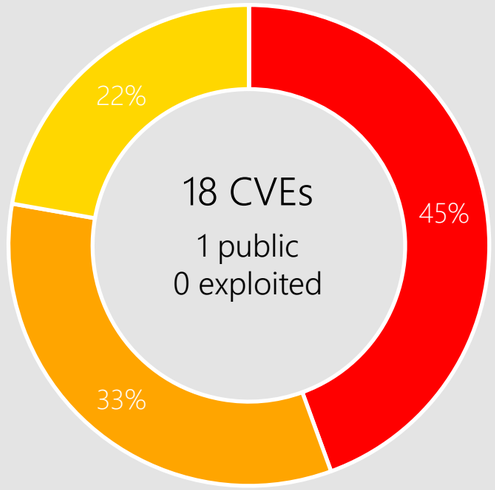
Windows 8.1, Server 2012 R2, and Server 2012



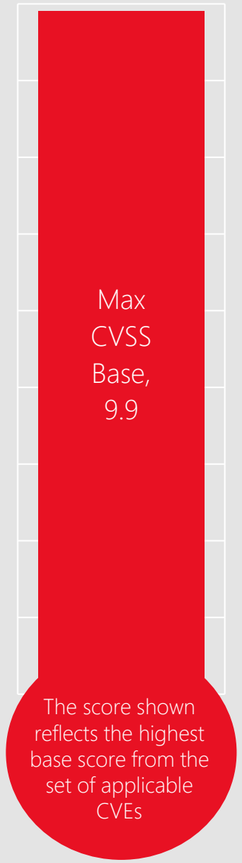
Windows 8.1 & Server 2012 R2



Windows Server 2012



Windows RT 8.1



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

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

Affected Components:

Bluetooth Driver
Digital TV Tuner device registration application
Event Tracing
Graphics Component
Font Parsing
LSA
Media MPEG-4 Video Decoder
Print Spooler
Remote Desktop Client
Scripting Engine
Services for NFS
ONCRPC XDR Driver
TCP/IP
User Account Profile
Picture

CVE-2021-26432 Services for NFS ONCRPC XDR Driver

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

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

CVE-2021-36942 LSA

Impact, Severity, Disclosure

Spoofing | Important | Publicly Disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

More Information

Additional steps are required if Active Directory Certificate Services (AD CS) is in your environment.
See ADV210003 Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS) for details

Affected Software

Server, version 20H2
Server, version 2004
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2021-34535 Remote Desktop Client

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

Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-34480 Scripting Engine

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 6.8 | Attack Vector: Network | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

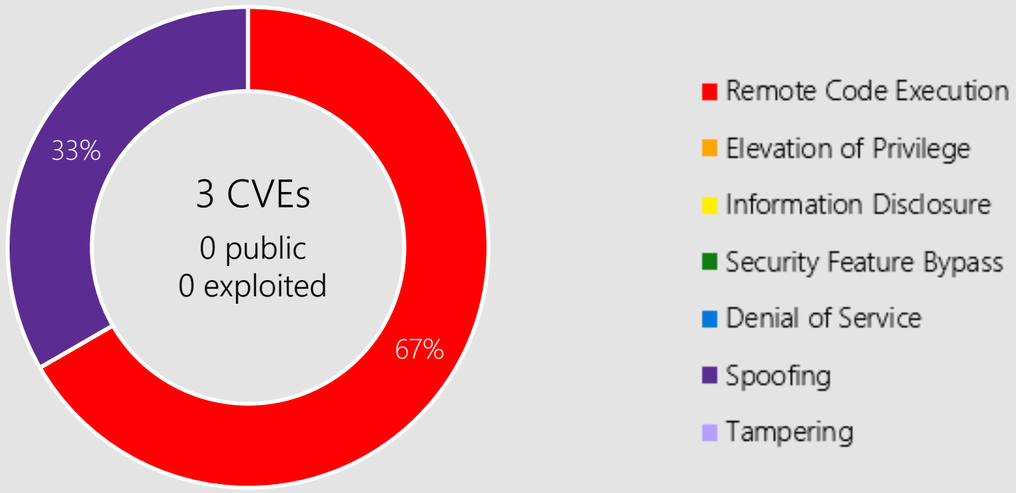
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac

CVE-2021-34478 Office

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

365 Apps Enterprise
Office 2019

CVE-2021-36941 Word

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

365 Apps Enterprise
Office 2019 for Mac

Other Products

Dynamics 365

CVE-2021-34524 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1

CVE-2021-36950 | 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 (on-premises) version 9.0.

Other Products

Dynamics Business Central/NAV

CVE-2021-36946 | 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 2019 Spring Update, Dynamics 365 Business Central 2020 Release Wave 1 - Update 16.15, Dynamics 365 Business Central 2020 Release Wave 2 - Update 17.9, Dynamics NAV 2017, Dynamics NAV 2018.

Other Products

.NET 5.0

CVE-2021-26423 | 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 5.0.

CVE-2021-34485 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET 5.0.

Other Products

.NET Core

CVE-2021-26423 | 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 2.1, .NET Core 3.1

CVE-2021-34485 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET Core 2.1, .NET Core 3.1

Other Products

.NET Core

CVE-2021-34532 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
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 2.1.

Other Products

Visual Studio

CVE-2021-26423 | 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 2019 version 16.10 (includes 16.0 - 16.9), Visual Studio 2019 for Mac version 8.10, Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)

CVE-2021-34485 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2019 version 16.10 (includes 16.0 - 16.9), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)

Other Products

Visual Studio

CVE-2021-34532 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2019 version 16.10 (includes 16.0 - 16.9), Visual Studio 2019 for Mac version 8.10, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6).

Other Products

Microsoft Malware Protection Engine

CVE-2021-34471 | 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: Malware Protection Engine.

Other Products

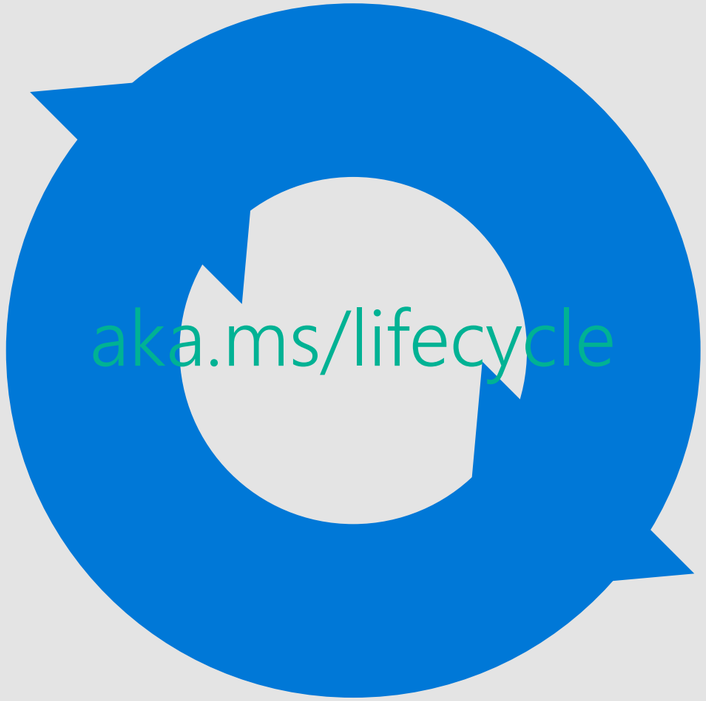
Azure

CVE-2021-33762/36943 Azure Cycle Cloud
CVE-2021-26428/26429/26430 Azure Sphere
CVE-2021-36949 Azure Active Directory Connect

Product Lifecycle Update

Products reaching end of support in August

.NET 2.1 Core (LTS)



Microsoft .NET and .NET Core releases

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	5001402	April 2021
Windows 10 1809/Server 2019	5005112	August 2021
Windows 10 1909/Windows Server, version 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-2021-34534	No	No	MSHTML Platform
CVE-2021-34486	No	No	Event Tracing
CVE-2021-34536	No	No	Storage Spaces Controller
CVE-2021-34487	No	No	Event Tracing
CVE-2021-34537	No	No	Bluetooth Driver
CVE-2021-26424	No	No	TCP/IP
CVE-2021-26425	No	No	Event Tracing
CVE-2021-26426	No	No	User Account Profile Picture
CVE-2021-36936	Yes	No	Print Spooler
CVE-2021-36937	No	No	Media MPEG-4 Video Decoder
CVE-2021-36938	No	No	Cryptographic Primitives Library
CVE-2021-36942	Yes	No	LSA
CVE-2021-36945	No	No	10 Update Assistant
CVE-2021-36947	No	No	Print Spooler

CVE	Public	Exploited	Product
CVE-2021-36948	No	Yes	Update Medic Service
CVE-2021-34471	No	No	Defender
CVE-2021-34530	No	No	Graphics Component
CVE-2021-34533	No	No	Graphics Component Font Parsing
CVE-2021-34483	No	No	Print Spooler
CVE-2021-34484	No	No	User Profile Service
CVE-2021-26431	No	No	Recovery Environment Agent
CVE-2021-26432	No	No	NFS ONCRPC XDR Driver
CVE-2021-26433	No	No	NFS ONCRPC XDR Driver
CVE-2021-36926	No	No	NFS ONCRPC XDR Driver
CVE-2021-36927	No	No	Digital TV Tuner device registration application
CVE-2021-36932	No	No	NFS ONCRPC XDR Driver
CVE-2021-36933	No	No	NFS ONCRPC XDR Driver
CVE-2021-30590	No	No	Chromium

CVE	Public	Exploited	Product
CVE-2021-30591	No	No	Chromium
CVE-2021-30592	No	No	Chromium
CVE-2021-30593	No	No	Chromium
CVE-2021-30594	No	No	Chromium
CVE-2021-30596	No	No	Chromium
CVE-2021-30597	No	No	Chromium
CVE-2021-34478	No	No	Office
CVE-2021-36940	No	No	SharePoint Server
CVE-2021-36941	No	No	Word
CVE-2021-33762	No	No	Azure CycleCloud
CVE-2021-34524	No	No	Dynamics 365 (on-premises)
CVE-2021-34480	No	No	Scripting Engine
CVE-2021-26423	No	No	.NET Core and Visual Studio
CVE-2021-26428	No	No	Azure Sphere

CVE	Public	Exploited	Product
CVE-2021-26429	No	No	Azure Sphere
CVE-2021-26430	No	No	Azure Sphere
CVE-2021-36946	No	No	Dynamics Business Central Cross-site Scripting
CVE-2021-36949	No	No	Azure Active Directory Connect Authentication Bypass
CVE-2021-36950	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2021-34532	No	No	ASP.NET Core and Visual Studio
CVE-2021-34485	No	No	.NET Core and Visual Studio
CVE-2021-34535	No	No	Remote Desktop Client
CVE-2021-36943	No	No	Azure CycleCloud