Microsoft

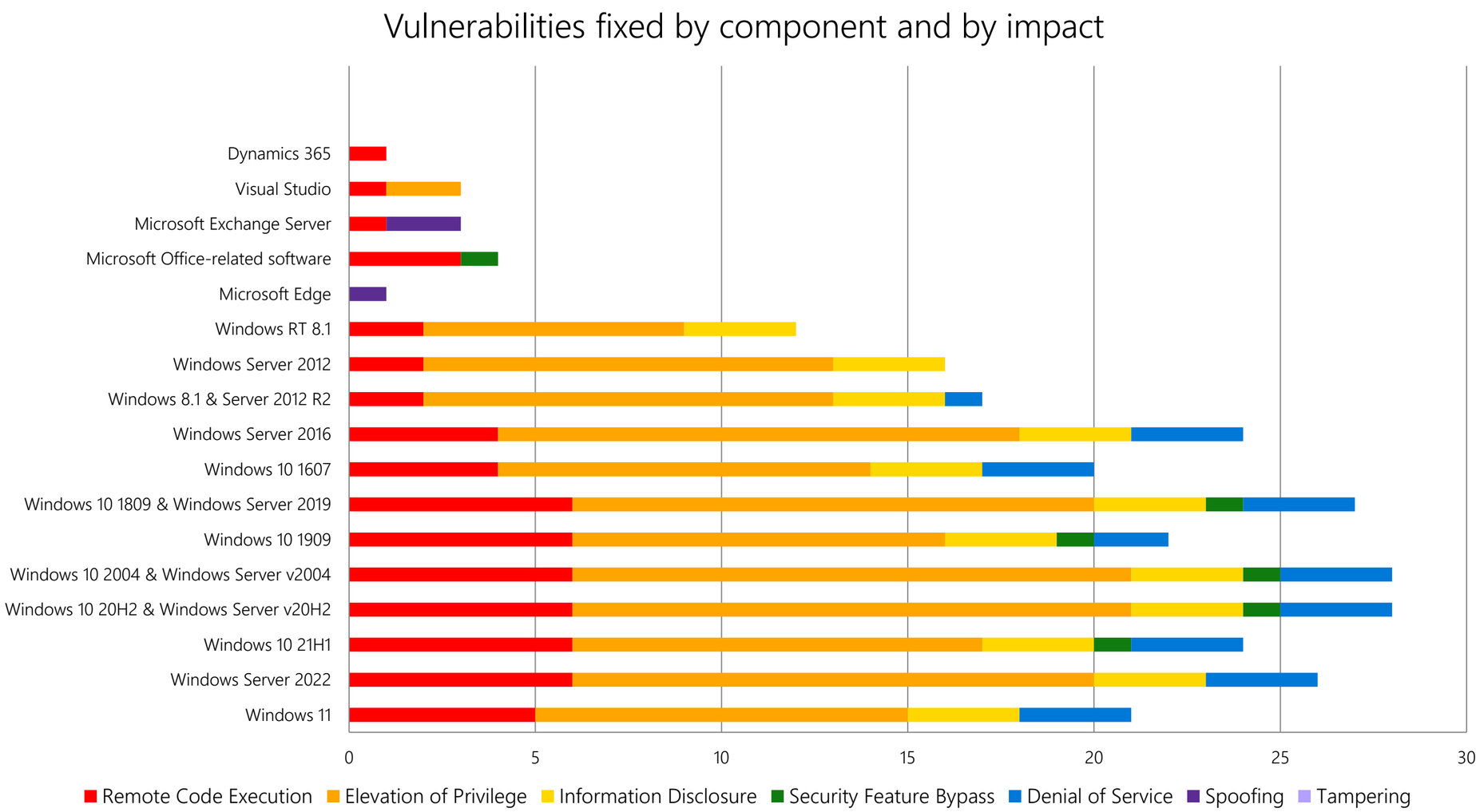
Microsoft Security Release

November 9, 2021

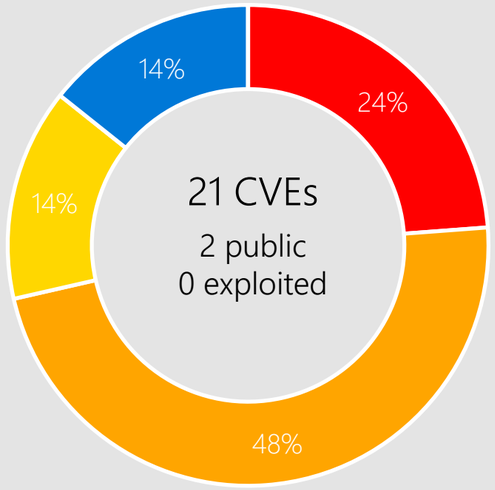
Agenda

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

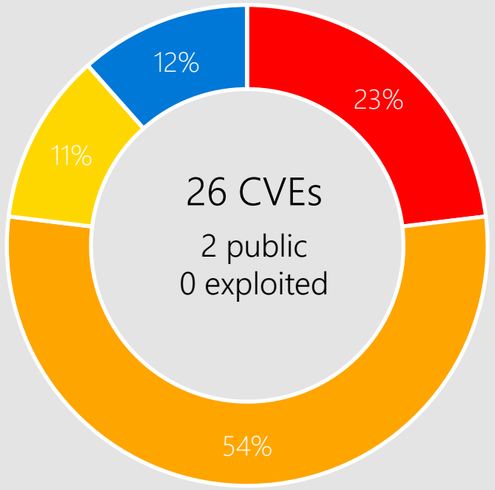
Monthly Security Release Overview - November 2021



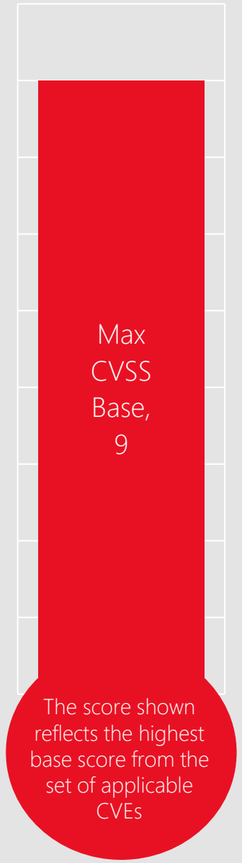
Windows 11, Server 2022



Windows 11



Windows Server 2022



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

Affected Components:

Active Directory Domain Services
Chakra Scripting Engine
COM
Credential Security Support Provider Protocol (CredSSP)
Desktop Bridge
Diagnostics Hub Standard Collector
Fast FAT File System Driver
Feedback Hub
Hyper-V
Hyper-V Discrete Device Assignment (DDA)
Installer
Kernel
Media Foundation
NTFS
Remote Desktop Client
Remote Desktop Protocol (RDP)
Remote Desktop Protocol Client
Virtual Machine Bus (VMBus)

CVE-2021-26443 Virtual Machine Bus (VMBus)

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

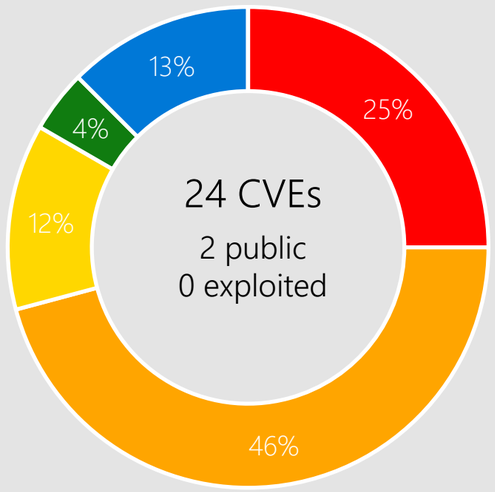
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

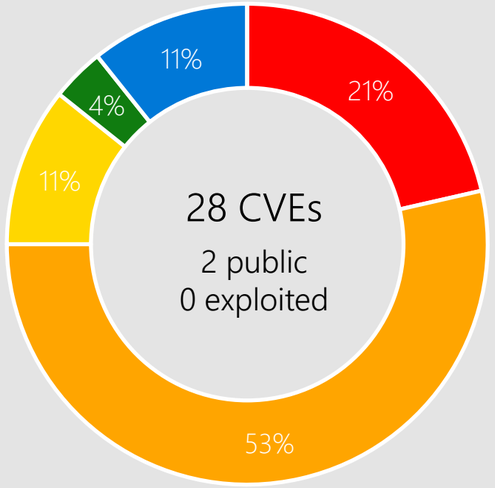
Affected Software

Windows 11
Server 2022
Server, version 20H2
Windows 10
Server, version 2004
Server 2019

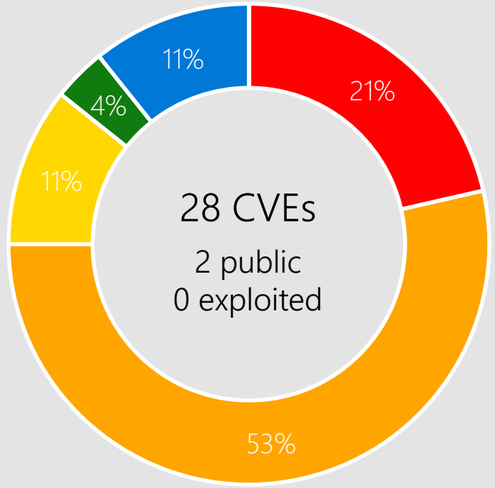
Windows 10



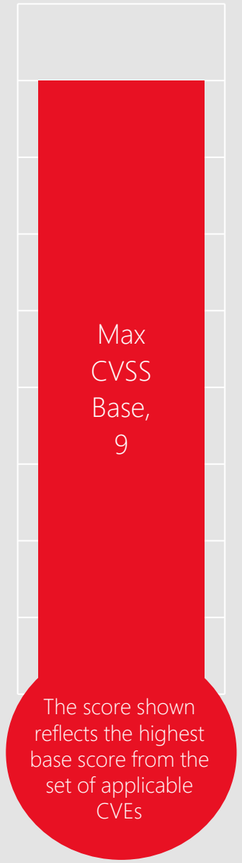
Windows 10 21H1



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:

Active Directory Domain Services
Chakra Scripting Engine
COM
Credential Security Support Provider Protocol (CredSSP)
Desktop Bridge
Diagnostics Hub Standard Collector
Fast FAT File System Driver
Feedback Hub
Hello
Hyper-V
Hyper-V Discrete Device Assignment (DDA)
Installer
Kernel
Media Foundation
NTFS
Remote Desktop Client
Remote Desktop Protocol (RDP)
Remote Desktop Protocol Client

CVE-2021-38666 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

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-2021-41378 NTFS

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: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

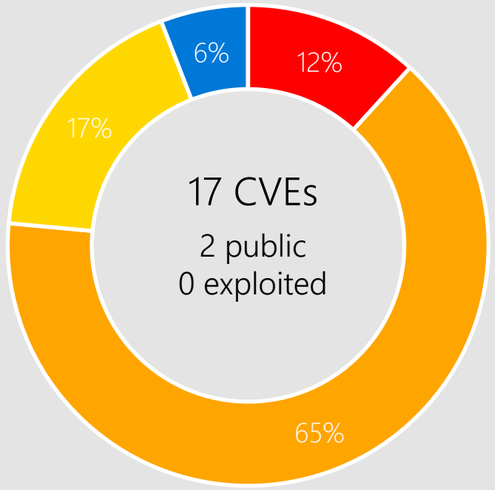
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

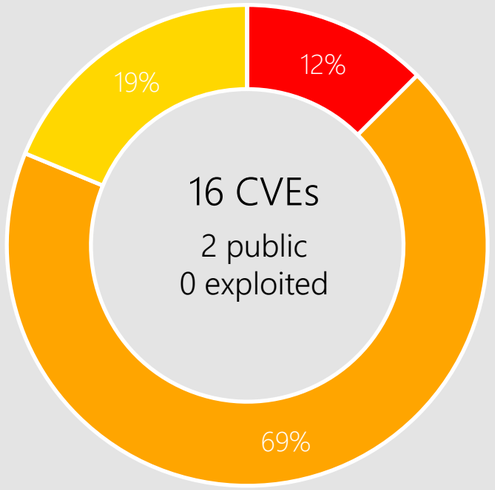
Affected Software

Windows 11
Server 2022
Server, version 20H2
Windows 10
Server, version 2004
Server 2019

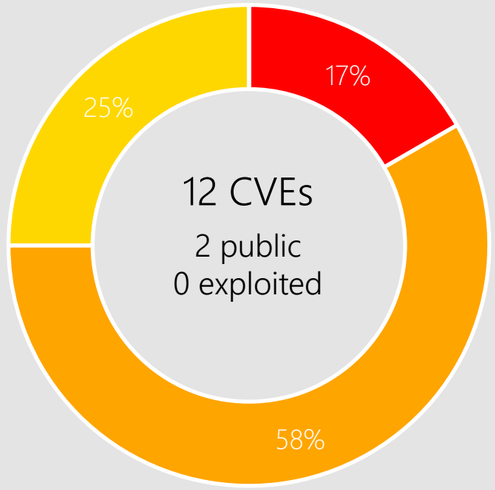
Windows 8.1, Server 2012 R2, and Server 2012



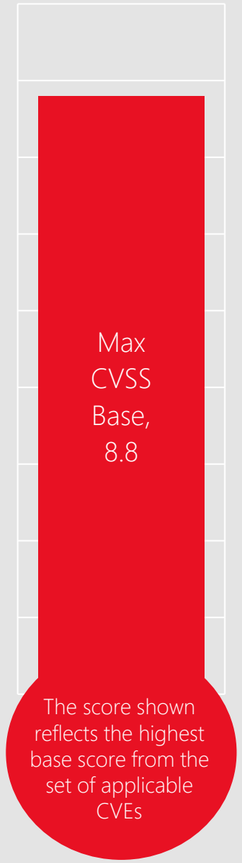
Windows 8.1 & Server 2012 R2



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:

Active Directory Domain Services
COM
Credential Security Support Provider Protocol (CredSSP)
Fast FAT File System Driver
Hyper-V
Installer
Kernel
NTFS
Remote Desktop Client

CVE-2021-42275 COM for Windows

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.

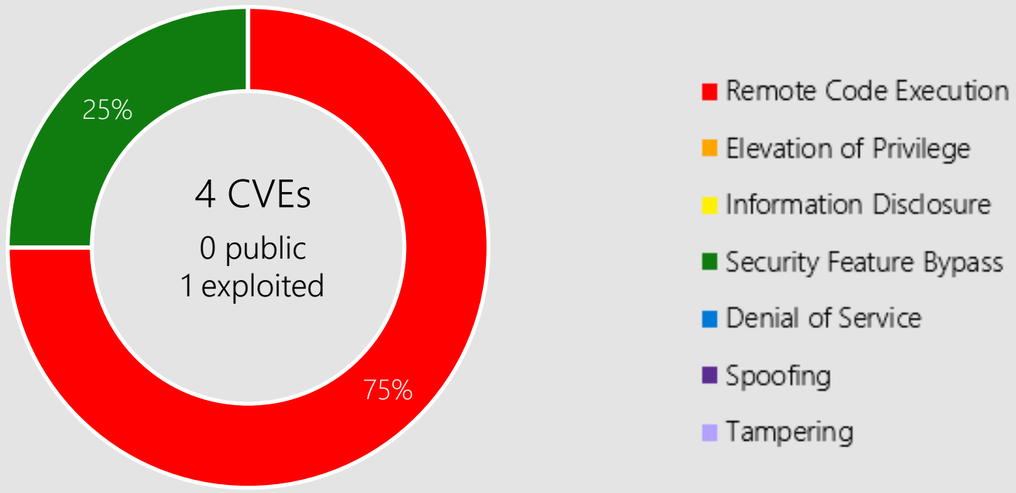
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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 Enterprise Server 2013
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013

CVE-2021-42292 Excel

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

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

CVE-2021-42296 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

Office LTSC 2021
365 Apps Enterprise

Other Products

Exchange Server

CVE-2021-42321 | Important | Remote Code Execution | Public: No | Exploited: Yes

CVSS Base Score 8.8
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

Exchange Server

CVE-2021-41349 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 21.

CVE-2021-42305 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 21.

Other Products

Dynamics 365

CVE-2021-42316 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.7
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Power BI Report Server

CVE-2021-41372 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Power BI Report Server.

Other Products

Visual Studio

CVE-2021-3711 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score unavailable as the vulnerability in Open SSL Software was not scored by the owning entity

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 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6).

CVE-2021-42277 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Windows 11, Server 2022, Server, version 20H2, Server, version 2004, Server 2019, Windows 10, Server 2016, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2015 Update 3, 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 16.7 (includes 16.0 – 16.6).

Other Products

Visual Studio

CVE-2021-42319 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 4.7
Attack Vector: Local
Attack Complexity: High
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 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6).

CVE-2021-42322 | 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 Code.

Other Products

Microsoft Malware Protection Engine

CVE-2021-42298 | Critical | 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: Malware Protection Engine.

Other Products

Azure and Mobile

CVE-2021-26444/42301/42302/42303/42304/42323 Azure RTOS
CVE-2021-41374/41375/41376/42300 Azure Sphere
CVE-2021-43208/43209 3D Viewer
CVE-2021-41373 FSLogix

Product Lifecycle Update

No fixed lifecycle products reaching end of support in November

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

Summary : Active Directory hardenings in Nov. 2021

Active Directory hardening included in Windows updates released on November 9, 2021

Please make sure to review those documents and take necessary actions.

NOTE: some changes will be enforced in the future updates.

- KB5008102—Active Directory Security Accounts Manager hardening changes (CVE-2021-42278)
- KB5008382—Verification of uniqueness for user principal name, service principal name, and the service principal name alias (CVE-2021-42282)
- KB5008380—Authentication updates (CVE-2021-42287)
- KB5008383—Active Directory permissions updates (CVE-2021-42291)

CVE	Public	Exploited	Product
CVE-2021-36957	No	No	Desktop Bridge
CVE-2021-38631	Yes	No	RDP
CVE-2021-41366	No	No	CredSSP
CVE-2021-41367	No	No	NTFS
CVE-2021-41371	Yes	No	RDP
CVE-2021-41377	No	No	Fast FAT File System Driver
CVE-2021-41378	No	No	NTFS
CVE-2021-41379	No	No	Installer
CVE-2021-26443	No	No	Virtual Machine Bus (VMBus)
CVE-2021-42274	No	No	Hyper-V Discrete Device Assignment (DDA)
CVE-2021-42275	No	No	COM for
CVE-2021-42276	No	No	Media Foundation
CVE-2021-42278	No	No	Active Directory Domain Services
CVE-2021-42279	No	No	Chakra Scripting Engine

CVE	Public	Exploited	Product
CVE-2021-42280	No	No	Feedback Hub
CVE-2021-38665	No	No	RDP Client
CVE-2021-38666	No	No	Remote Desktop Client
CVE-2021-41356	No	No	Windows
CVE-2021-41370	No	No	NTFS
CVE-2021-42277	No	No	Diagnostics Hub Standard Collector
CVE-2021-42282	No	No	AD Domain Services
CVE-2021-42283	No	No	NTFS
CVE-2021-42284	No	No	Hyper-V
CVE-2021-42285	No	No	Kernel
CVE-2021-42286	No	No	Core Shell SI Host Extension Framework for Composable Shell
CVE-2021-42287	No	No	Active Directory Domain Services
CVE-2021-42288	No	No	Windows Hello
CVE-2021-42291	No	No	AD Domain Services

CVE	Public	Exploited	Product
CVE-2021-42298	No	No	Defender
CVE-2021-41351	No	No	Edge (Chrome based) on IE Mode
CVE-2021-41368	No	No	Access
CVE-2021-40442	No	No	Excel
CVE-2021-42292	No	Yes	Excel
CVE-2021-42296	No	No	Word
CVE-2021-41349	No	No	Exchange Server
CVE-2021-3711	No	No	OpenSSL: CVE-2021-3711 SM2 Decryption Buffer Overflow
CVE-2021-41372	No	No	Power BI Report Server
CVE-2021-42300	No	No	Azure Sphere
CVE-2021-42301	No	No	Azure RTOS
CVE-2021-42302	No	No	Azure RTOS
CVE-2021-42303	No	No	Azure RTOS
CVE-2021-42304	No	No	Azure RTOS

CVE	Public	Exploited	Product
CVE-2021-42316	No	No	Dynamics 365 (on-premises)
CVE-2021-42319	No	No	Visual Studio
CVE-2021-42322	No	No	Visual Studio Code
CVE-2021-43208	Yes	No	3D Viewer
CVE-2021-43209	Yes	No	3D Viewer
CVE-2021-41373	No	No	FSLogix
CVE-2021-41374	No	No	Azure Sphere
CVE-2021-41375	No	No	Azure Sphere
CVE-2021-41376	No	No	Azure Sphere
CVE-2021-42305	No	No	Exchange Server
CVE-2021-42321	No	Yes	Exchange Server
CVE-2021-42323	No	No	Azure RTOS
CVE-2021-26444	No	No	Azure RTOS