Microsoft

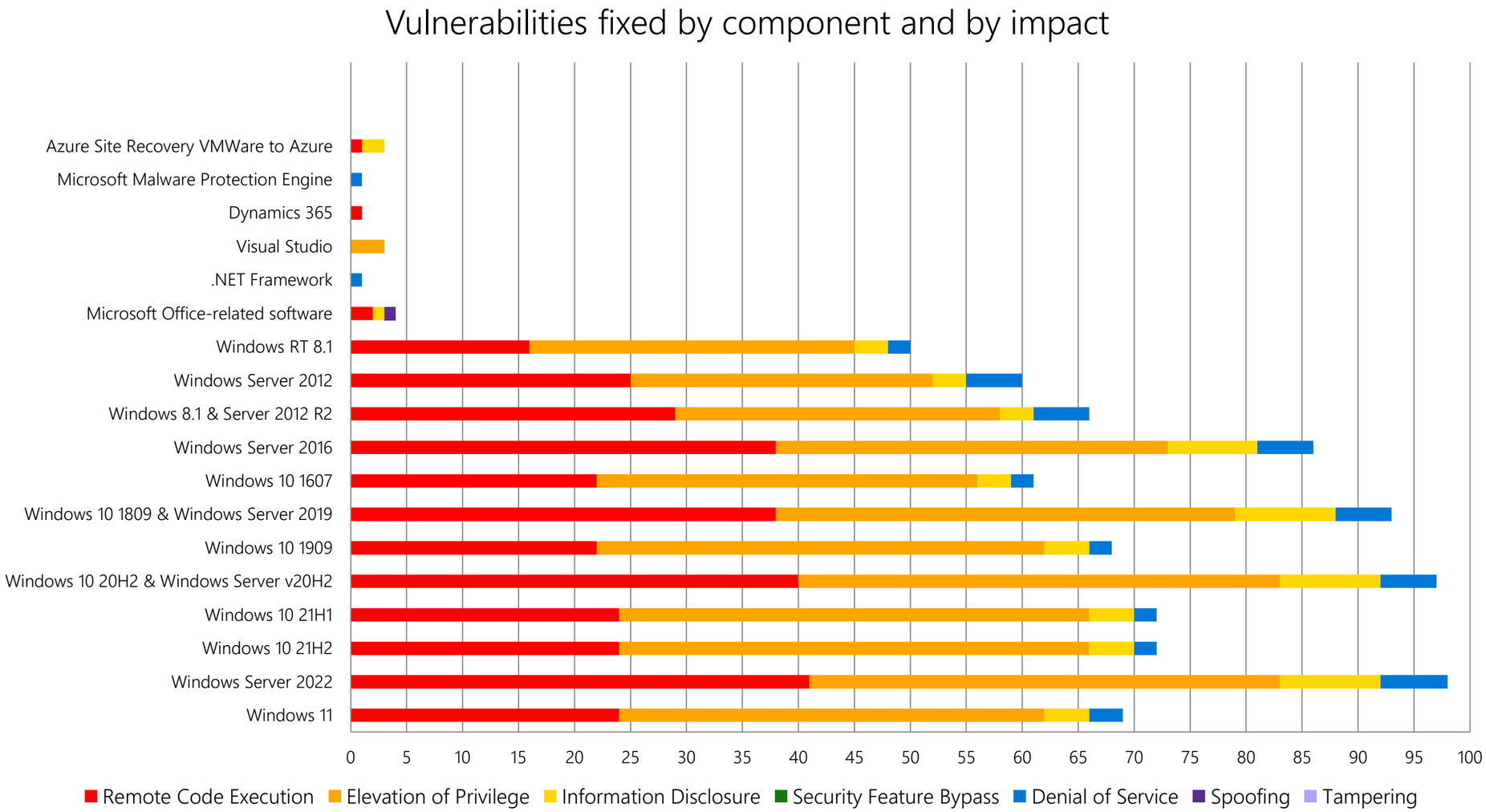
Microsoft Security Release

April 12, 2022

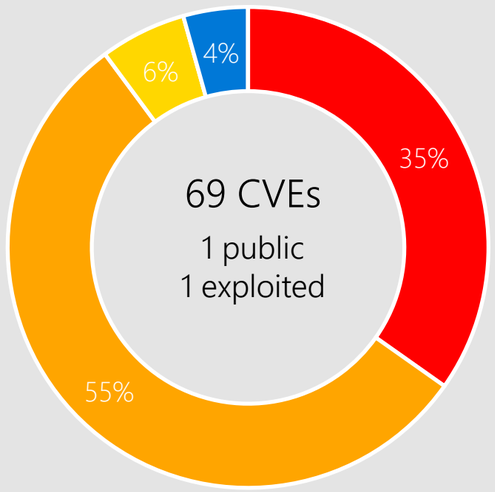
Agenda

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

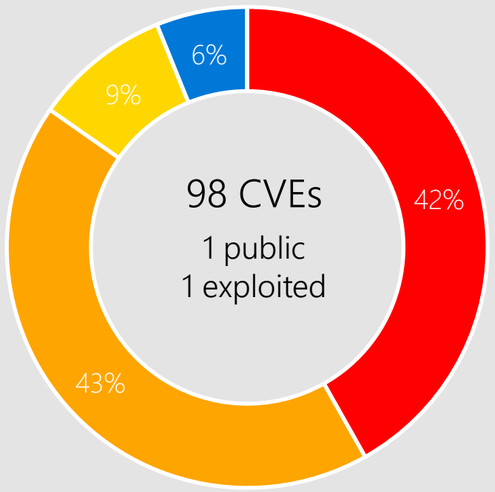
Monthly Security Release Overview - April 2022



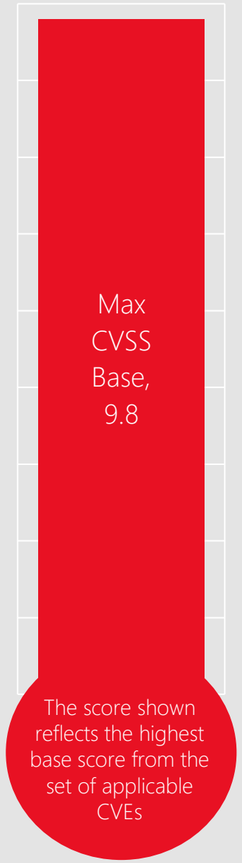
Windows 11, Server 2022



Windows 11



Windows Server 2022



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

Affected Components:

Please see Appendix for complete list.

CVE-2022-26809 RPC Runtime

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

Block TCP port 445 at the perimeter firewall

Follow Microsoft guidelines to secure SMB traffic https://docs.microsoft.com/windows-server/storage/file-server/smb-secure-traffic

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

CVE-2022-24491 Network File System

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

NFS Role must be enabled for a system to be vulnerable to this attack.

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

CVE-2022-24541 Server Service

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

Block TCP port 445 at the perimeter firewall

Follow Microsoft guidelines to secure SMB traffic https://docs.microsoft.com/windows-server/storage/file-server/smb-secure-traffic

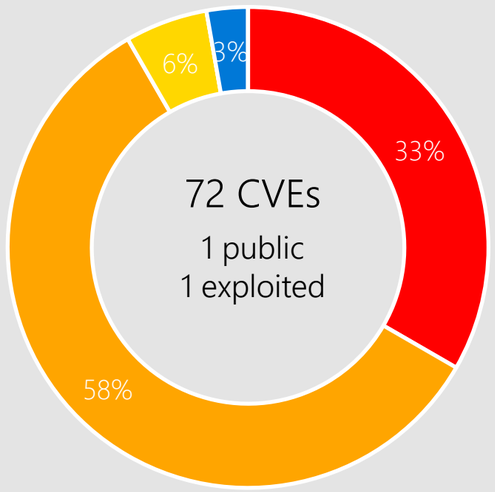
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

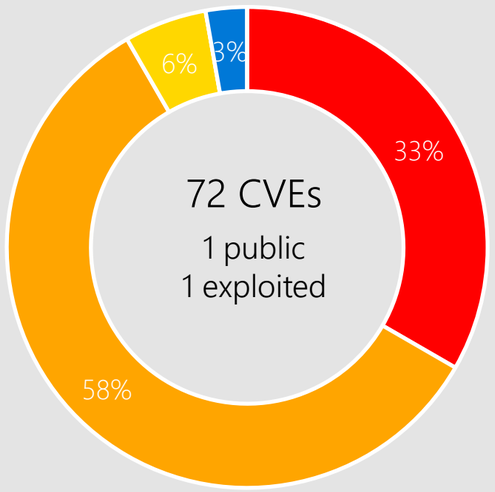
Affected Software

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

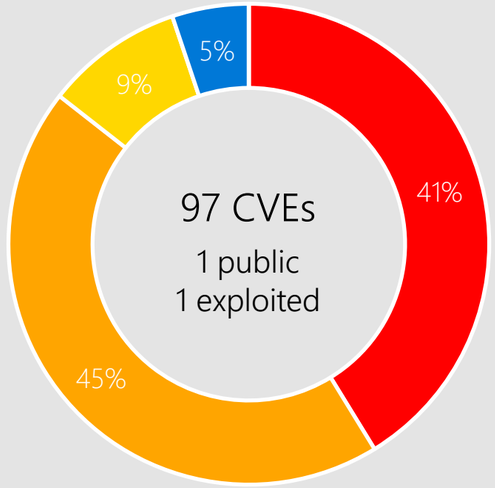
Windows 10



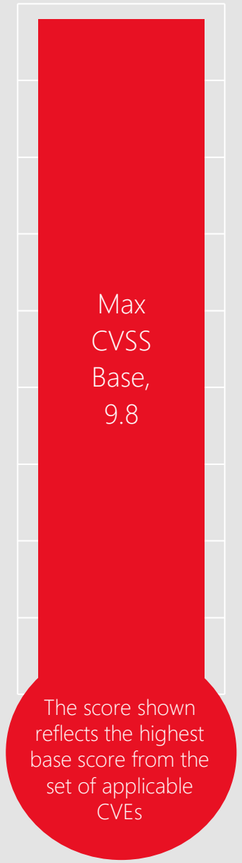
Windows 10 21H2



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:

Please see Appendix for complete list.

CVE-2022-24500 SMB

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

Block TCP port 445 at the perimeter firewall

Follow Microsoft guidelines to secure SMB traffic https://docs.microsoft.com/windows-server/storage/file-server/smb-secure-traffic

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

CVE-2022-23257 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | 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
Windows 10
Server, version 20H2

CVE-2022-24487 Local Security Authority (LSA)

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.

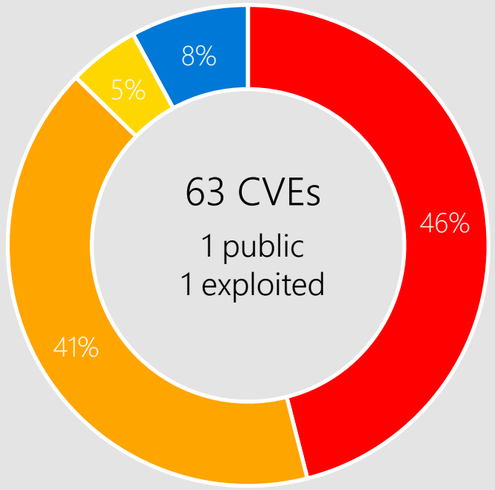
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

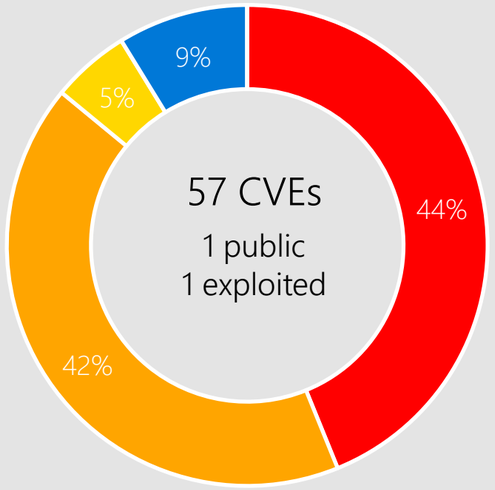
Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016

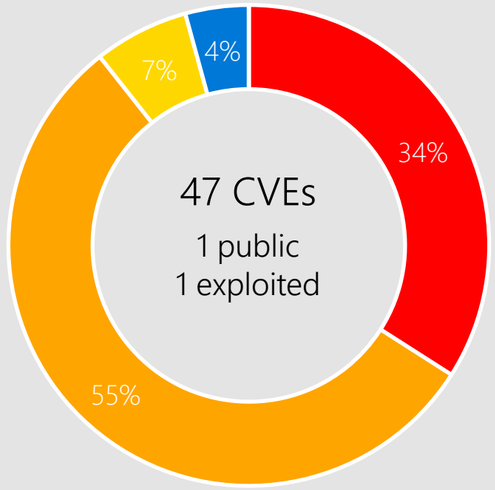
Windows 8.1, Server 2012 R2, and Server 2012



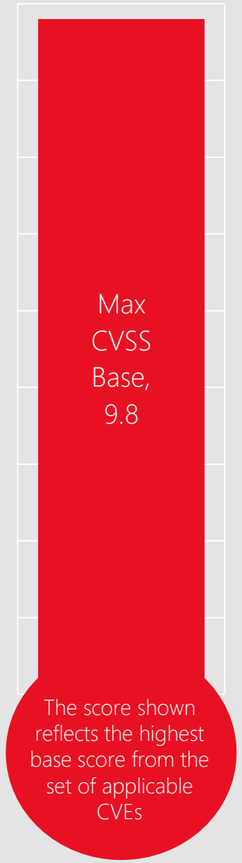
Windows 8.1 & Server 2012 R2



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:

Please see Appendix for complete list.

CVE-2022-24533 Remote Desktop Protocol

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8 | 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

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

CVE-2022-24521 CLFS

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately Disclosed | 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

CVE-2022-26904 User Profile Service

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7 | Attack Vector: Local | Attack Complexity: High | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

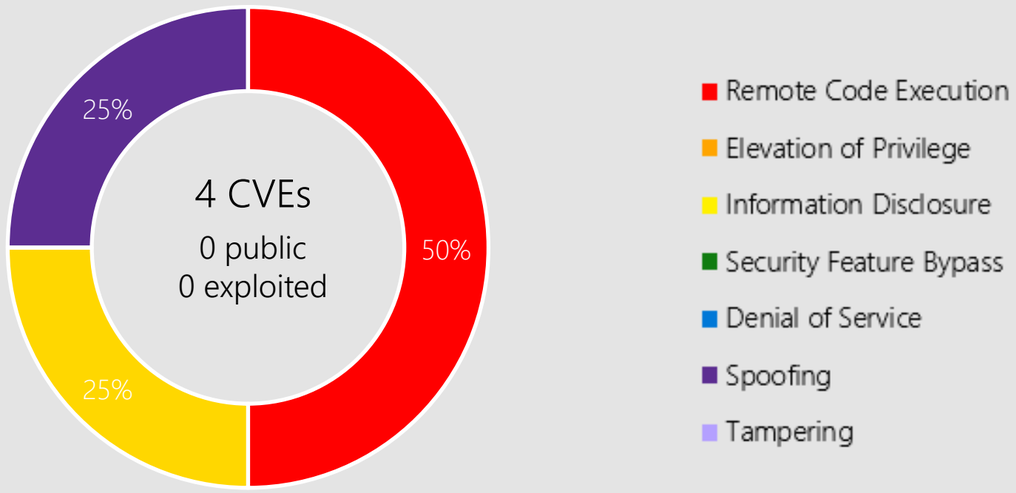
Workarounds

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 2013/2016/2019
Excel 2013/2016
SharePoint Server 2016/2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Lync Server 2013 CU10
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
Skype Business Server 2015 CU12
Skype Business Server 2019 CU6

CVE-2022-26901 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

Office 2016
Excel 2016
SharePoint Server Subscription Edition
Excel 2013
SharePoint Foundation 2013
Office Web Apps Server 201
Office 2013
Office 2019 for Mac
Office 2019
SharePoint Enterprise Server 2016
Office Online Server
Office LTSC 2021
Office LTSC for Mac 2021
365 Apps Enterprise

CVE-2022-24472 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8 | 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 Server 2016
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Enterprise Server 2016
SharePoint Server 2019

Other Products

Dynamics 365

CVE-2022-23259 | 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: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

Other Products

.NET Framework

CVE-2022-26832 | 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 Framework 2.0, 3.0, 4.6 on Server 2008, .NET Framework 3.5 on Windows 8.1, .NET Framework 4.8 on Windows 8.1 x64-based systems, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.8 on Server, version 20H2, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Windows 11, .NET Framework 4.5.2 on Windows 8.1, .NET Framework 4.5.2 on Windows 8.1, .NET Framework 4.8 on Windows 10 21H2, .NET Framework 4.8 on Windows 10 21H1, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 4.5.2 on Server 2012 R2, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.8 on Server 2012, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 x64-based systems, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.5.2 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 10 1909, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 32-bit systems, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Windows 8.1, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 4.5.2 on Server 2012, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 4.8 on Windows 8.1 32-bit systems, .NET Framework 4.5.2 on Server 2008, .NET Framework 4.8 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 10 20H2.

Other Products

Visual Studio

CVE-2022-24513 | 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 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.1, Visual Studio 2019 for Mac version 8.10, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8).

CVE-2022-26921 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio Code

Other Products

Visual Studio

CVE-2022-24767 | Important | Elevation of Privilege | Public: No | Exploited: No

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 2022 version 17.0, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6).

CVE-2022-24765 | Important | Elevation of Privilege | Public: No | Exploited: No

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 2022 version 17.0, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.7 (includes 16.0 – 16.6).

Other Products

Microsoft Malware Protection Engine

CVE-2022-24548 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Malware Protection Engine.

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-26898 | 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.

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-26896 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 4.9
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

CVE-2022-26897 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 4.9
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

Other Products

Power BI, Azure SDK, YARP

CVE-2022-23292 Power BI
CVE-2022-26907 Azure SDK for .NET
CVE-2022-26924 YARP

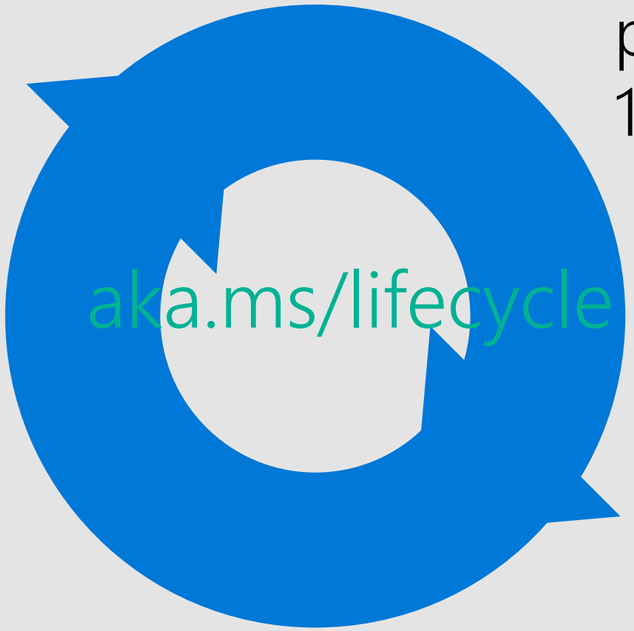
Product Lifecycle Update

Products reaching end of support

.NET Framework 4.5.2
.NET Framework 4.6
.NET Framework 4.6.1

Modern policy – release end of servicing

Dynamics 365 Business Central on-premises, 2020 release wave 2, version 17.x



Upcoming end of servicing for Windows 10 1909, 20H2*: May 10, 2022

*20H2 Home, Pro, Pro Education, Pro for Workstations only

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5012672	April 2022
Windows Server 2012	5013270	April 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-2022-22008	No	No	Hyper-V
CVE-2022-22009	No	No	Hyper-V
CVE-2022-21983	No	No	Win32 Stream Enumeration
CVE-2022-23257	No	No	Hyper-V
CVE-2022-23268	No	No	Hyper-V
CVE-2022-24521	No	Yes	Common Log File System Driver
CVE-2022-24474	No	No	Win32k
CVE-2022-24484	No	No	Cluster Shared Volume (CSV)
CVE-2022-24533	No	No	Remote Desktop Protocol
CVE-2022-24485	No	No	Win32 File Enumeration
CVE-2022-24534	No	No	Win32 Stream Enumeration
CVE-2022-24486	No	No	Kerberos
CVE-2022-24544	No	No	Kerberos
CVE-2022-24496	No	No	Local Security Authority (LSA)

CVE	Public	Exploited	Product
CVE-2022-24545	No	No	Kerberos
CVE-2022-24548	No	No	Defender
CVE-2022-24549	No	No	AppX Package Manager
CVE-2022-24500	No	No	SMB
CVE-2022-24550	No	No	Telephony Server
CVE-2022-26786	No	No	Print Spooler
CVE-2022-26787	No	No	Print Spooler
CVE-2022-26788	No	No	PowerShell
CVE-2022-26789	No	No	Print Spooler
CVE-2022-26790	No	No	Print Spooler
CVE-2022-26791	No	No	Print Spooler
CVE-2022-26792	No	No	Print Spooler
CVE-2022-26793	No	No	Print Spooler
CVE-2022-26794	No	No	Print Spooler

CVE	Public	Exploited	Product
CVE-2022-26795	No	No	Print Spooler
CVE-2022-26796	No	No	Print Spooler
CVE-2022-26797	No	No	Print Spooler
CVE-2022-26798	No	No	Print Spooler
CVE-2022-26811	No	No	DNS Server
CVE-2022-26812	No	No	DNS Server
CVE-2022-26813	No	No	DNS Server
CVE-2022-26904	Yes	No	User Profile Service
CVE-2022-26914	No	No	Win32k
CVE-2022-26915	No	No	Secure Channel
CVE-2022-26916	No	No	Fax Compose Form
CVE-2022-26917	No	No	Fax Compose Form
CVE-2022-26918	No	No	Fax Compose Form
CVE-2022-26919	No	No	LDAP

CVE	Public	Exploited	Product
CVE-2022-26920	No	No	Graphics Component
CVE-2022-24527	No	No	Endpoint Configuration Manager
CVE-2022-24479	No	No	Connected User Experiences and Telemetry
CVE-2022-24528	No	No	Remote Procedure Call Runtime
CVE-2022-24481	No	No	Common Log File System Driver
CVE-2022-24530	No	No	Installer
CVE-2022-24482	No	No	ALPC
CVE-2022-24532	No	No	HEVC Video Extensions
CVE-2022-24483	No	No	Kernel
CVE-2022-24487	No	No	Local Security Authority (LSA)
CVE-2022-24536	No	No	DNS Server
CVE-2022-24488	No	No	Desktop Bridge
CVE-2022-24537	No	No	Hyper-V
CVE-2022-24489	No	No	Cluster Client Failover (CCF)

CVE	Public	Exploited	Product
CVE-2022-24538	No	No	Cluster Shared Volume (CSV)
CVE-2022-24490	No	No	Hyper-V Shared Virtual Hard Disks
CVE-2022-24539	No	No	Hyper-V Shared Virtual Hard Disks
CVE-2022-24491	No	No	Network File System
CVE-2022-24540	No	No	ALPC
CVE-2022-24492	No	No	Remote Procedure Call Runtime
CVE-2022-24541	No	No	Server Service
CVE-2022-24542	No	No	Win32k
CVE-2022-24494	No	No	Ancillary Function Driver for WinSock
CVE-2022-24543	No	No	Upgrade Assistant
CVE-2022-24495	No	No	Direct Show -
CVE-2022-24497	No	No	Network File System
CVE-2022-24546	No	No	DWM Core Library
CVE-2022-24498	No	No	iSCSI Target Service

CVE	Public	Exploited	Product
CVE-2022-24547	No	No	Digital Media Receiver
CVE-2022-24499	No	No	Installer
CVE-2022-26783	No	No	Hyper-V Shared Virtual Hard Disks
CVE-2022-26784	No	No	Cluster Shared Volume (CSV)
CVE-2022-26785	No	No	Hyper-V Shared Virtual Hard Disks
CVE-2022-26801	No	No	Print Spooler
CVE-2022-26802	No	No	Print Spooler
CVE-2022-26803	No	No	Print Spooler
CVE-2022-26807	No	No	Work Folder Service
CVE-2022-26808	No	No	File Explorer
CVE-2022-26809	No	No	Remote Procedure Call Runtime
CVE-2022-26810	No	No	File Server Resource Management Service
CVE-2022-26814	No	No	DNS Server
CVE-2022-26815	No	No	DNS Server

CVE	Public	Exploited	Product
CVE-2022-26816	No	No	DNS Server
CVE-2022-26817	No	No	DNS Server
CVE-2022-26818	No	No	DNS Server
CVE-2022-26819	No	No	DNS Server
CVE-2022-26820	No	No	DNS Server
CVE-2022-26821	No	No	DNS Server
CVE-2022-26822	No	No	DNS Server
CVE-2022-26823	No	No	DNS Server
CVE-2022-26824	No	No	DNS Server
CVE-2022-26825	No	No	DNS Server
CVE-2022-26826	No	No	DNS Server
CVE-2022-26827	No	No	File Server Resource Management Service
CVE-2022-26828	No	No	Bluetooth Driver
CVE-2022-26829	No	No	DNS Server

CVE	Public	Exploited	Product
CVE-2022-26830	No	No	DiskUsage.exe
CVE-2022-26831	No	No	LDAP
CVE-2022-26903	No	No	Graphics Component
CVE-2022-24765	No	No	GitHub: Uncontrolled search for the Git directory in Git for
CVE-2022-24767	No	No	GitHub: Git for ' uninstaller vulnerable to DLL hijacking when run under the SYSTEM user account

CVE	Public	Exploited	Product
CVE-2022-24473	No	No	Excel
CVE-2022-26901	No	No	Excel
CVE-2022-24472	No	No	SharePoint Server
CVE-2022-26910	No	No	Skype for Business and Lync
CVE-2022-26911	No	No	Skype for Business
CVE-2022-23292	No	No	Power BI
CVE-2022-24513	No	No	Visual Studio
CVE-2022-26896	No	No	Azure Site Recovery
CVE-2022-26897	No	No	Azure Site Recovery
CVE-2022-26898	No	No	Azure Site Recovery
CVE-2022-23259	No	No	Dynamics 365 (on-premises)
CVE-2022-24493	No	No	Local Security Authority (LSA) Server

CVE	Public	Exploited	Product
CVE-2022-26832	No	No	.NET Framework
CVE-2022-26907	No	No	Azure SDK for .NET
CVE-2022-26921	No	No	Visual Studio Code
CVE-2022-26924	No	No	YARP