Microsoft

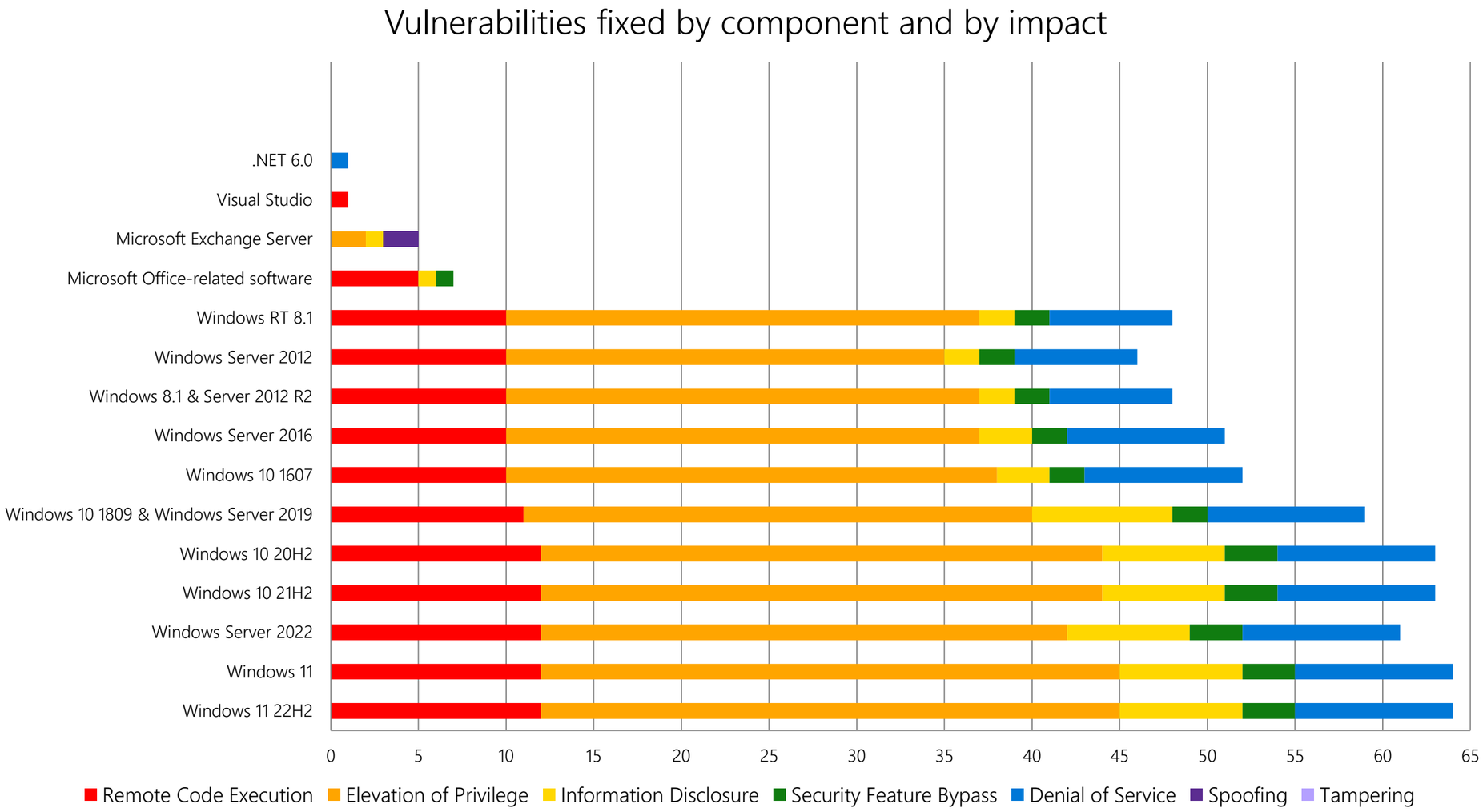
Microsoft Security Release

January 10, 2023

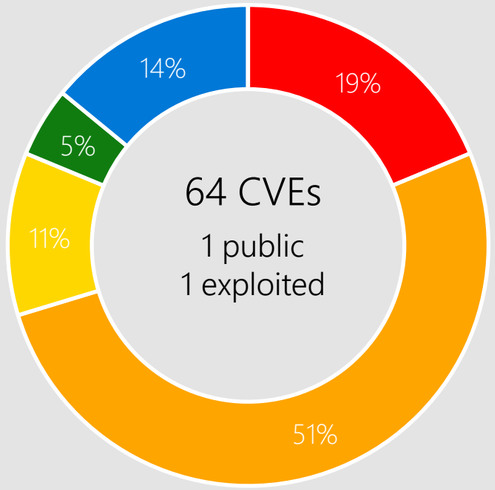
Agenda

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

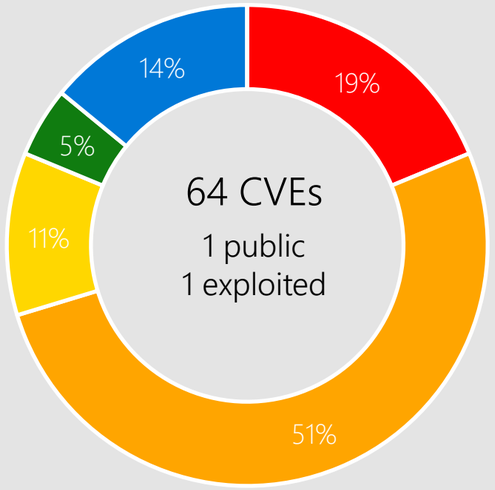
Monthly Security Release Overview - January 2023



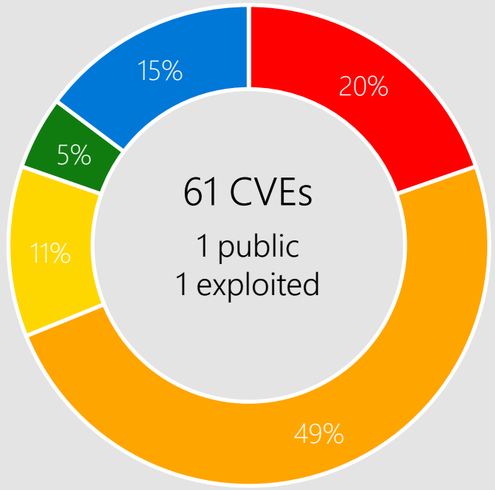
Windows 11, Server 2022



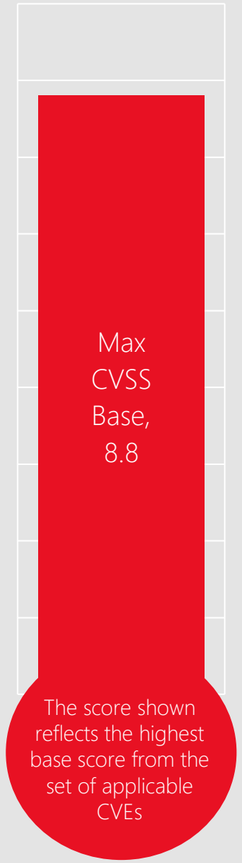
Windows 11 22H2



Windows 11



Windows Server 2022



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:

Please see Appendix for complete list

CVE-2023-21674 Advanced Local Procedure Call (ALPC)

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Windows 8.1

CVE-2023-21549 SMB Witness Service

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

CVE-2023-21561 Cryptographic Services

Impact, Severity, Disclosure

Elevation of Privilege | 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.

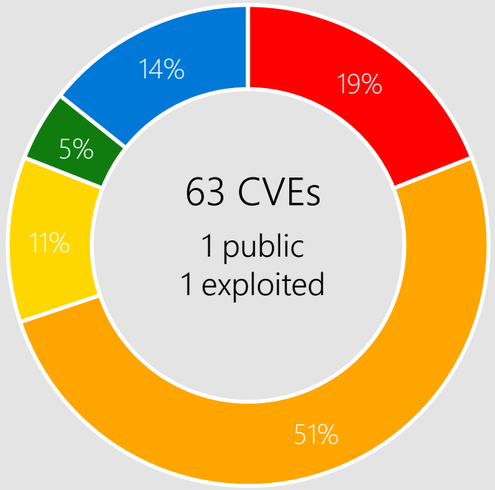
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

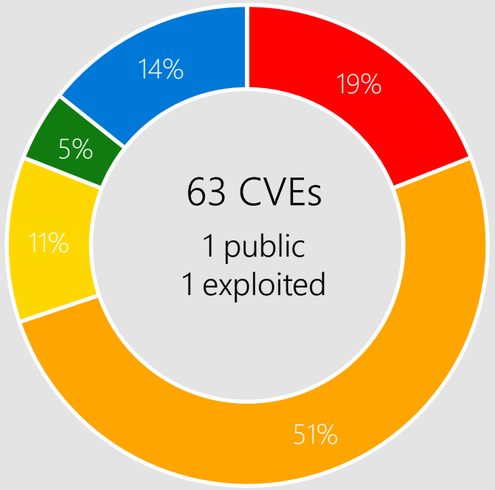
Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

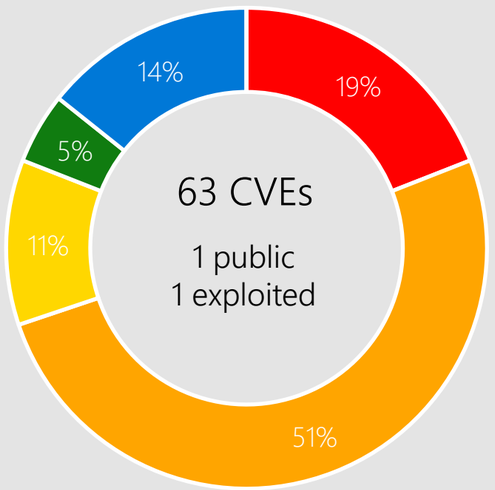
Windows 10



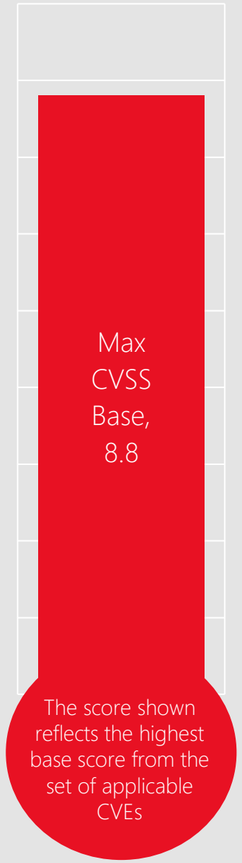
Windows 10 22H2



Windows 10 21H2



Windows 10 20H2



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-2023-21676 LDAP

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 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10

CVE-2023-21681 WDAC OLE DB Provider

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: 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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

CVE-2023-21535 SSTP

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.

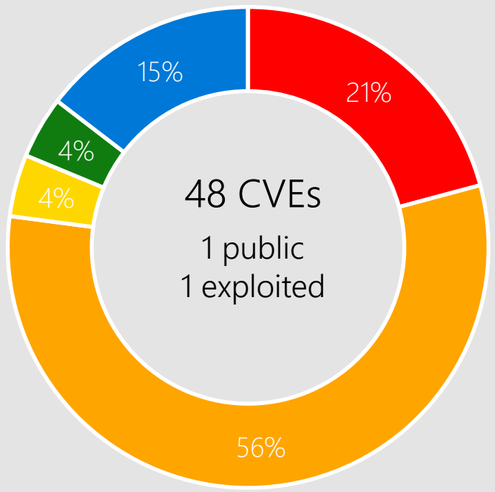
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

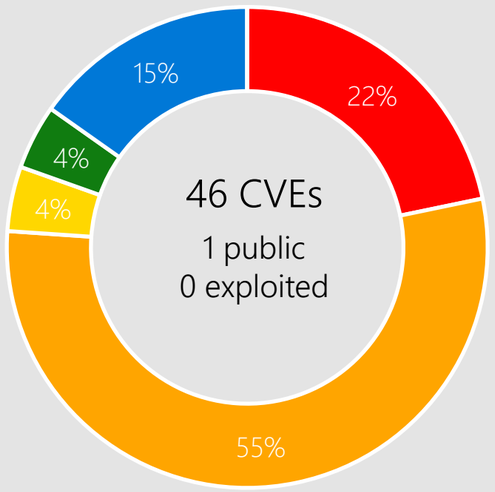
Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

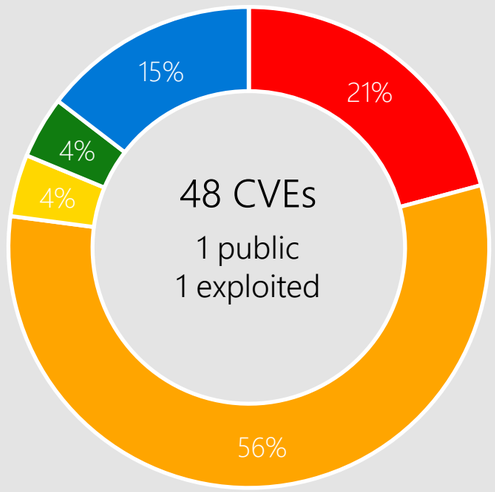
Windows 8.1, Server 2012 R2, and Server 2012



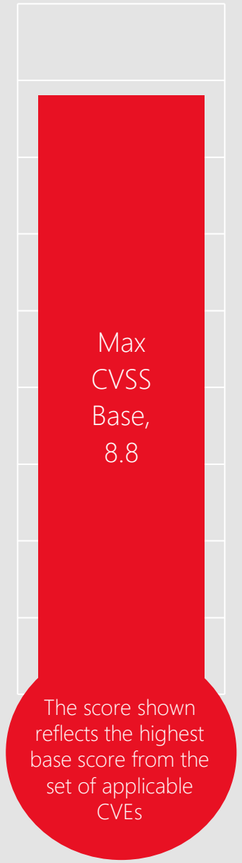
Windows 8.1 & Server 2012 R2



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-2023-21543 Layer 2 Tunneling Protocol (L2TP)

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.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

CVE-2023-21732 ODBC Driver

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: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

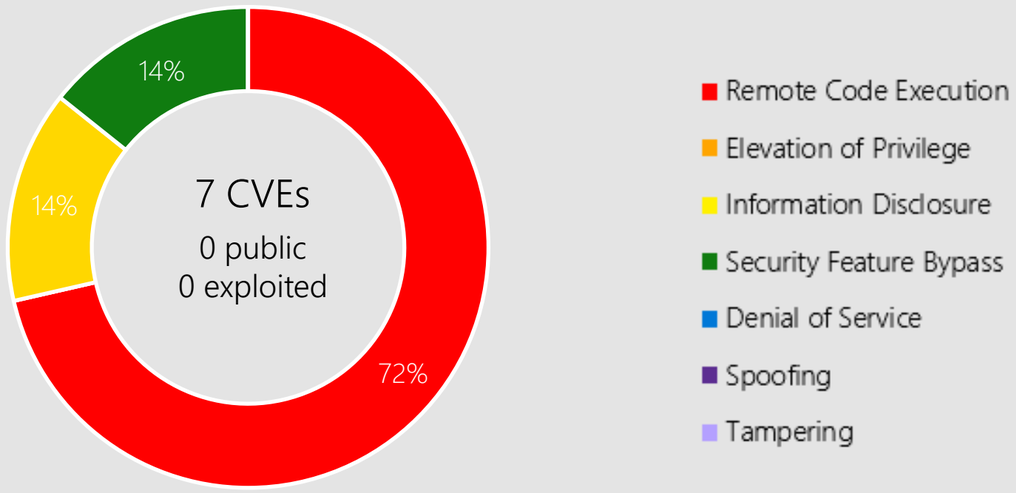
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- 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
Office LTSC for Mac 2021
Office LTSC 2021
SharePoint Foundation 2013
SharePoint Server Subscription Edition
Visio 2013
Visio 2016

CVE-2023-21742 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 2019
SharePoint Server Subscription Edition
SharePoint Enterprise Server 2016
SharePoint Enterprise Server 2013

CVE-2023-21734 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

Office LTSC for Mac 2021
365 Apps Enterprise
Office 2019 for Mac

Other Products

Exchange Server

CVE-2023-21763 | 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: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 11.

CVE-2023-21764 | 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: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 11.

Other Products

Exchange Server

CVE-2023-21745 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

CVE-2023-21762 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

Other Products

Exchange Server

CVE-2023-21761 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 23.

Other Products

.NET 6.0

CVE-2023-21538 | 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 6.0.

Other Products

Visual Studio

CVE-2023-21779 | Important | Remote Code Execution | 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

Azure, Store Apps, and Malicious Software Removal Tool

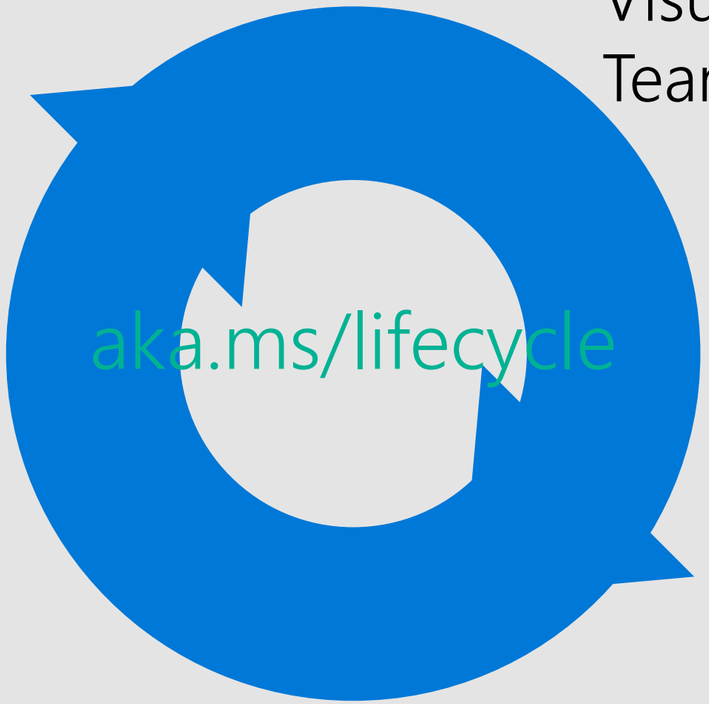
CVE-2023-21725 Malicious Software Removal Tool
CVE-2023-21531 Azure Service Fabric
CVE-2023-21780-21793 3D Builder

Product Lifecycle Update

Products reaching end of support in January

Windows 8.1
Dynamics AX 2012 R3
Dynamics NAV 2013/2013 R2

Visual Studio 2012
Team Foundation Server 2012



[Latest Servicing Stack Updates]

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-21524	No	No	LSA
CVE-2023-21532	No	No	GDI
CVE-2023-21535	No	No	SSTP
CVE-2023-21546	No	No	L2TP
CVE-2023-21547	No	No	Internet Key Exchange (IKE) Protocol
CVE-2023-21539	No	No	Authentication
CVE-2023-21540	No	No	Cryptographic
CVE-2023-21541	No	No	Task Scheduler
CVE-2023-21542	No	No	Installer
CVE-2023-21543	No	No	L2TP
CVE-2023-21548	No	No	SSTP
CVE-2023-21549	Yes	No	Workstation Service
CVE-2023-21550	No	No	Cryptographic
CVE-2023-21551	No	No	Cryptographic Services

CVE	Public	Exploited	Product
CVE-2023-21552	No	No	GDI
CVE-2023-21555	No	No	L2TP
CVE-2023-21556	No	No	L2TP
CVE-2023-21557	No	No	Lightweight Directory Access Protocol (LDAP)
CVE-2023-21558	No	No	Error Reporting Service
CVE-2023-21559	No	No	Cryptographic Services
CVE-2023-21560	No	No	Boot Manager
CVE-2023-21561	No	No	Cryptographic Services
CVE-2023-21563	No	No	BitLocker
CVE-2023-21674	No	Yes	Advanced Local Procedure Call (ALPC)
CVE-2023-21676	No	No	LDAP
CVE-2023-21677	No	No	Internet Key Exchange (IKE) Extension
CVE-2023-21678	No	No	Print Spooler
CVE-2023-21679	No	No	L2TP

CVE	Public	Exploited	Product
CVE-2023-21680	No	No	Win32k
CVE-2023-21682	No	No	Point-to-Point Protocol (PPP)
CVE-2023-21683	No	No	Internet Key Exchange (IKE) Extension
CVE-2023-21724	No	No	DWM Core Library
CVE-2023-21725	No	No	Malicious Software Removal Tool
CVE-2023-21726	No	No	Credential Manager User Interface
CVE-2023-21728	No	No	Netlogon
CVE-2023-21730	No	No	Cryptographic Services
CVE-2023-21732	No	No	ODBC Driver
CVE-2023-21733	No	No	Bind Filter Driver
CVE-2023-21739	No	No	Bluetooth Driver
CVE-2023-21746	No	No	NTLM
CVE-2023-21747	No	No	Kernel
CVE-2023-21748	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-21749	No	No	Kernel
CVE-2023-21750	No	No	Kernel
CVE-2023-21752	No	No	Backup Service
CVE-2023-21753	No	No	Event Tracing for
CVE-2023-21754	No	No	Kernel
CVE-2023-21755	No	No	Kernel
CVE-2023-21757	No	No	Layer 2 Tunneling Protocol (L2TP)
CVE-2023-21758	No	No	Internet Key Exchange (IKE) Extension
CVE-2023-21759	No	No	Smart Card Resource Management Server
CVE-2023-21760	No	No	Print Spooler
CVE-2023-21765	No	No	Print Spooler
CVE-2023-21766	No	No	Overlay Filter
CVE-2023-21767	No	No	Overlay Filter
CVE-2023-21768	No	No	Ancillary Function Driver for WinSock

CVE	Public	Exploited	Product
CVE-2023-21771	No	No	Local Session Manager (LSM)
CVE-2023-21772	No	No	Kernel
CVE-2023-21773	No	No	Kernel
CVE-2023-21774	No	No	Kernel
CVE-2023-21776	No	No	Kernel
CVE-2023-21525	No	No	Encrypting File System (EFS)
CVE-2023-21527	No	No	iSCSI Service
CVE-2023-21536	No	No	Event Tracing for
CVE-2023-21675	No	No	Kernel
CVE-2023-21734	No	No	Office
CVE-2023-21735	No	No	Office
CVE-2023-21736	No	No	Office Visio
CVE-2023-21737	No	No	Office Visio
CVE-2023-21738	No	No	Office Visio

CVE	Public	Exploited	Product
CVE-2023-21741	No	No	Office Visio
CVE-2023-21742	No	No	SharePoint Server
CVE-2023-21743	No	No	SharePoint Server
CVE-2023-21744	No	No	SharePoint Server
CVE-2023-21538	No	No	.NET
CVE-2023-21681	No	No	WDAC OLE DB provider for SQL Server
CVE-2023-21761	No	No	Exchange Server
CVE-2023-21762	No	No	Exchange Server
CVE-2023-21763	No	No	Exchange Server
CVE-2023-21764	No	No	Exchange Server
CVE-2023-21780	No	No	3D Builder
CVE-2023-21781	No	No	3D Builder
CVE-2023-21782	No	No	3D Builder
CVE-2023-21784	No	No	3D Builder

CVE	Public	Exploited	Product
CVE-2023-21786	No	No	3D Builder
CVE-2023-21791	No	No	3D Builder
CVE-2023-21793	No	No	3D Builder
CVE-2023-21531	No	No	Azure Service Fabric Container
CVE-2023-21537	No	No	Message Queuing (MSMQ)
CVE-2023-21745	No	No	Exchange Server
CVE-2023-21779	No	No	Visual Studio Code
CVE-2023-21783	No	No	3D Builder
CVE-2023-21785	No	No	3D Builder
CVE-2023-21787	No	No	3D Builder
CVE-2023-21788	No	No	3D Builder
CVE-2023-21789	No	No	3D Builder
CVE-2023-21790	No	No	3D Builder
CVE-2023-21792	No	No	3D Builder