Microsoft

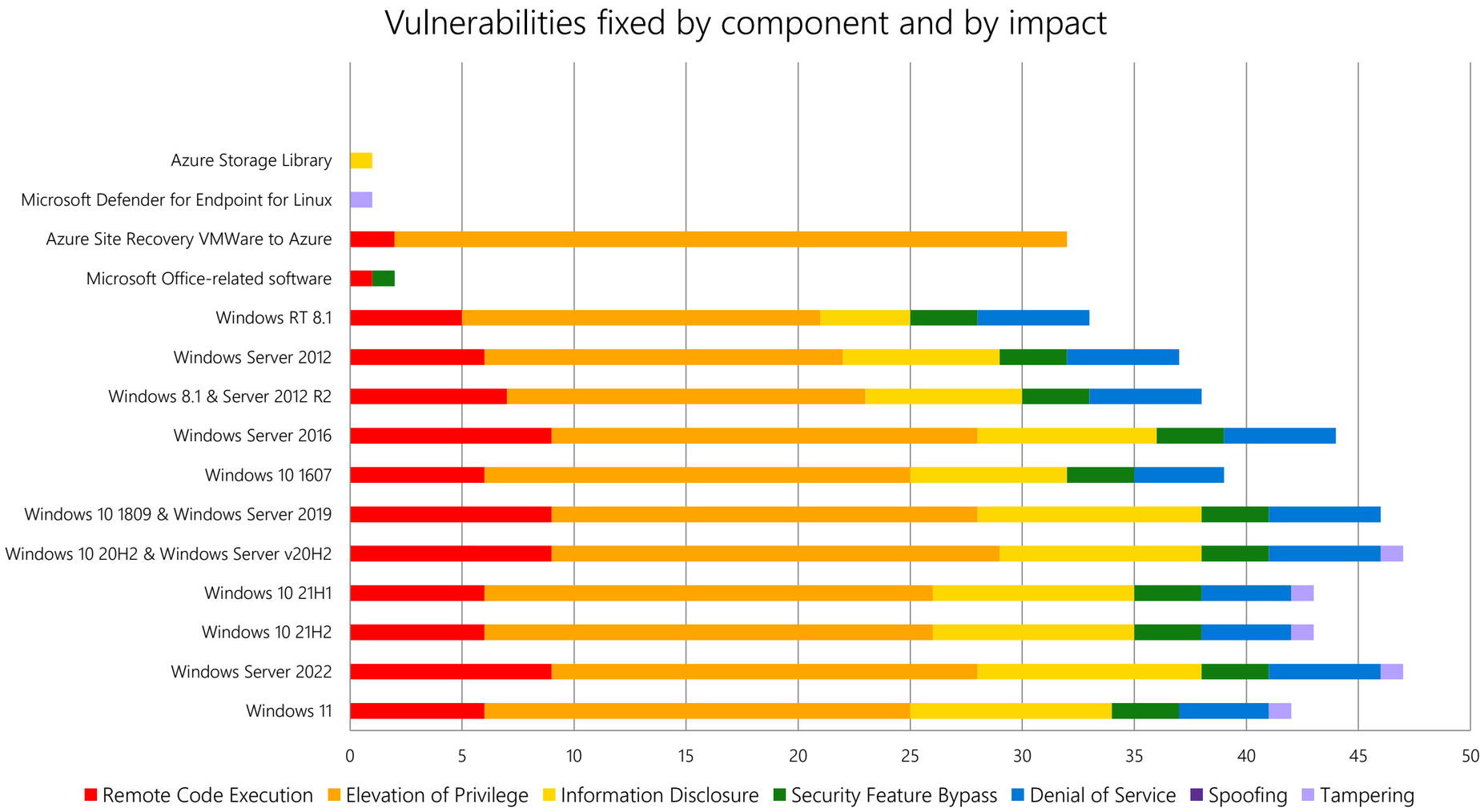
Microsoft Security Release

July 12, 2022

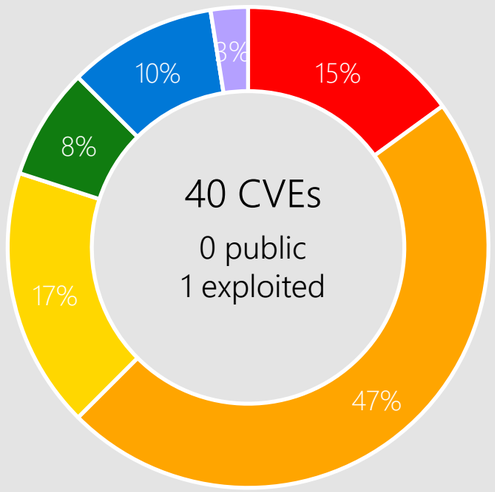
Agenda

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

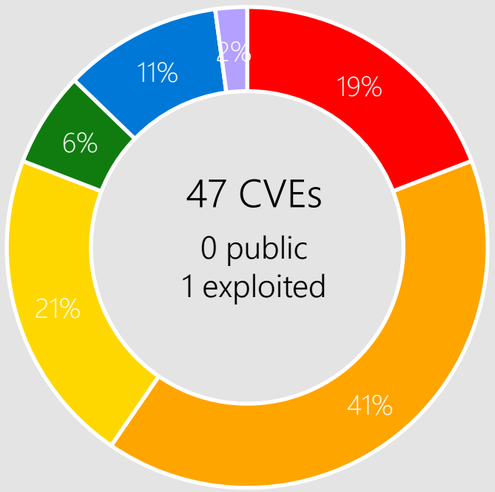
Monthly Security Release Overview - July 2022



Windows 11, Server 2022

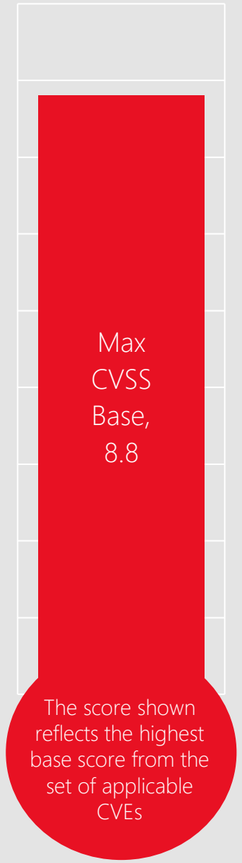


Windows 11



Windows Server 2022

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



Affected Components:

See appendix for details

CVE-2022-30216 Server Service

Impact, Severity, Disclosure

Tampering | 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
Windows 10

CVE-2022-22047 CSRSS

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.

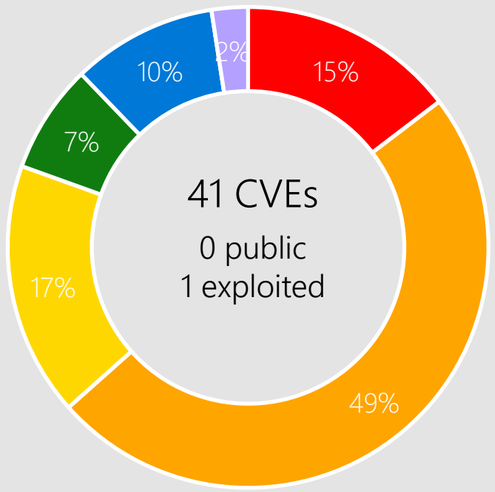
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

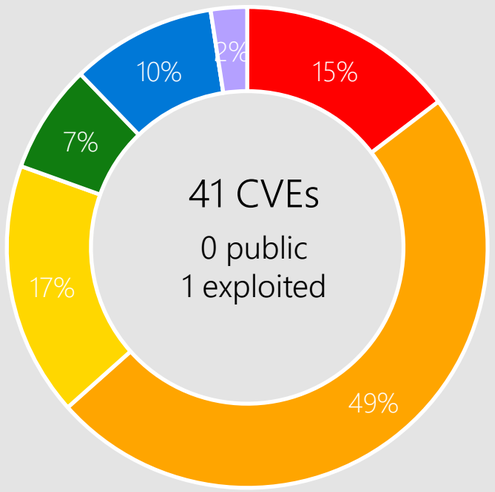
Affected Software

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

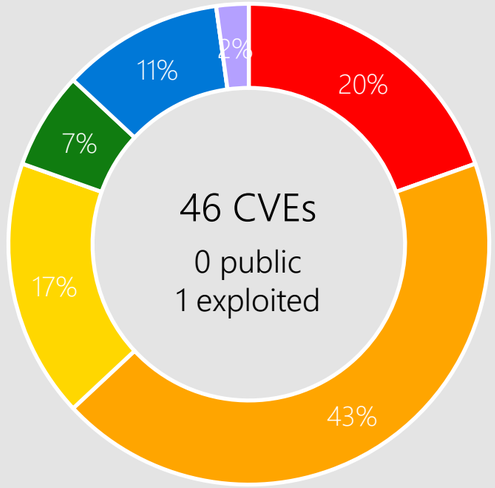
Windows 10



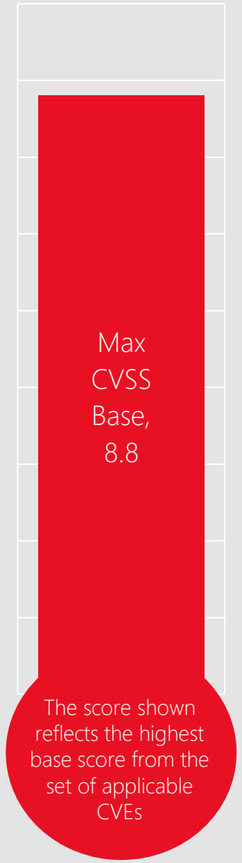
Windows 10 21H2



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:

See appendix for details

CVE-2022-23825 and 23816 AMD

Impact, Severity, Disclosure

Information Disclosure| Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Please see AMD security bulletin https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1037

More Information

Customers who allow untrusted users to execute arbitrary code might wish to implement some extra security features within their systems. These features protect against the intra-process disclosure vectors that this speculative execution vulnerability describes. See the following for more information.

Windows client: https://support.microsoft.com/help/4073119
Windows Server/Azure Stack HCI: https://support.microsoft.com/help/4072698

Affected Software

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

CVE-2022-22026 CSRSS

Impact, Severity, Disclosure

Elevation of Privilege | Important | 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
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-30221 Graphics Component

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.

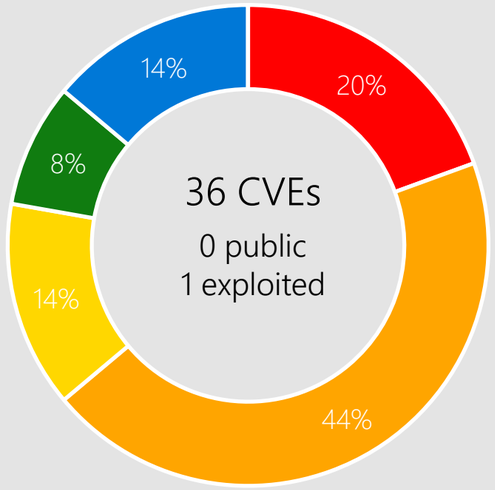
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

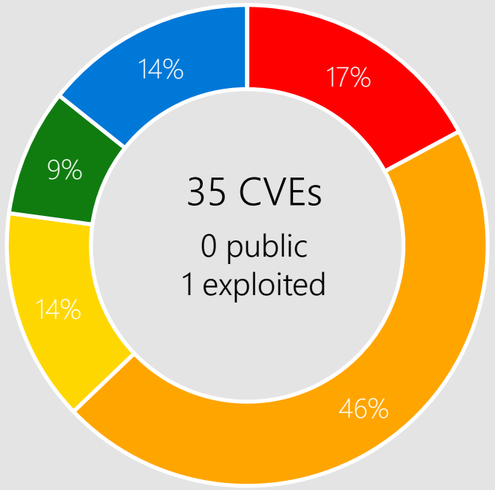
Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Windows 8.1
RD Client for Windows Desktop

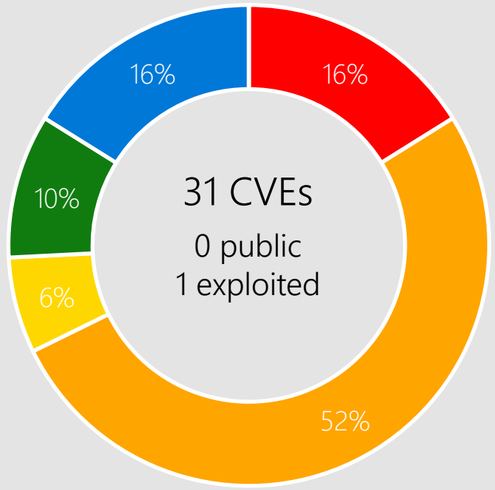
Windows 8.1, Server 2012 R2, and Server 2012



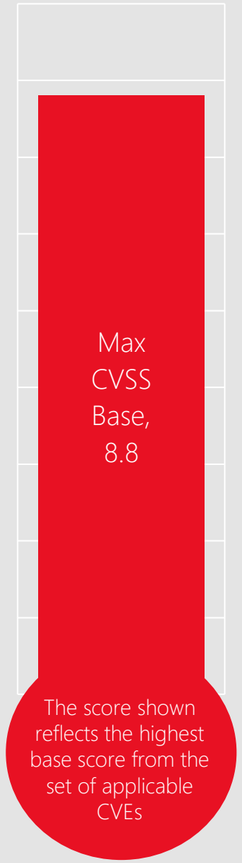
Windows 8.1 & Server 2012 R2



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:

Advanced LPC
BitLocker
Boot Manager
CLFS Driver

CSRSS
Fast FAT File System Driver
Fax Service

GDI+
Graphics Component
Group Policy
Hyper-V

IIS Server
IIS Cachuri Module
IIS Dynamic Compression Module

Kernel
L2TP
Media Player Network Sharing Service
NFS

Portable Device Enumerator Service

Print Spooler

CVE-2022-22038 Remote Procedure Call Runtime

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

CVE-2022-22029 Network File System

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

This vulnerability is not exploitable in NFSV4.1

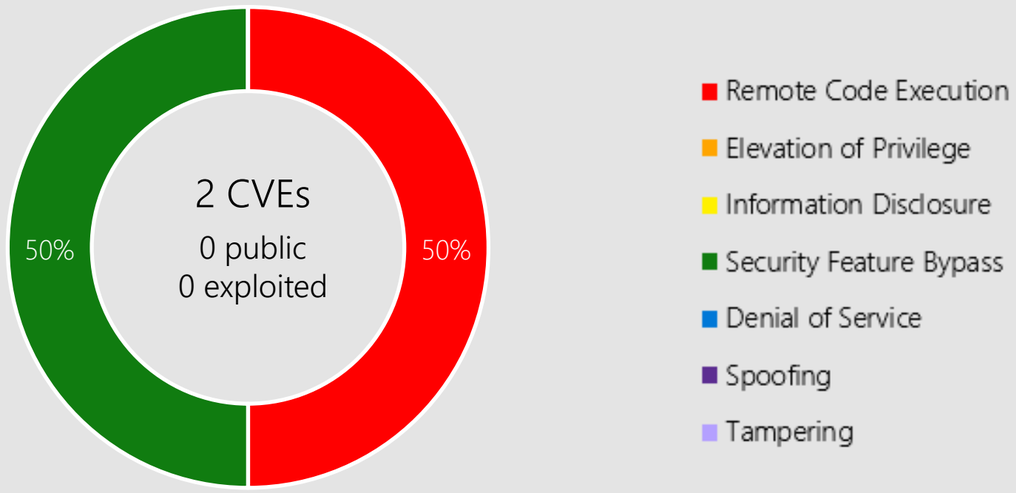
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server, version 20H2
Server 2019
Server 2016
Server 2012 R2
Server 2012

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
365 Apps Enterprise
Lync Server 2013 CU10
Office LTSC 2021
Skype Business Server 2015 CU12
Skype Business Server 2019 CU6

CVE-2022-33633 Skype for Business and Lync

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | 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

Skype Business Server 2019 CU6
Skype Business Server 2015 CU12
Lync Server 2013 CU10

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-33674 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.3
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

CVE-2022-33675 | 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: Azure Site Recovery VMWare to Azure.

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-33676/33678 | 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.

CVE-2022-33677 | Important | Elevation of Privilege | 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-2022-30181/33641/33643/33655-33657/33661-33663/33665-33667/33672/33673 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

CVE-2022-33642/33650/33651/33653/33654/33659/33660/33664/33668/33669/33671 | Important | Elevation of Privilege | 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

Azure Site Recovery VMWare to Azure

CVE-2022-33652/33658 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 4.4
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

Other Products

Azure Storage Library

CVE-2022-30187 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 4.7
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Azure Storage Library Python Queue Storage SDK, Azure Storage Library Python Blob Storage SDK, Azure Storage Library Java Blob Storage, Azure Storage Library .NET Blob Storage SDK, Azure Storage Library Java Queue Storage SDK, Azure Storage Library .NET Queue Storage SDK

More Information: See Azure Storage Blog for details on implementation: http://aka.ms/azstorageclientencryptionblog

Other Products

Microsoft Defender for Endpoint for Linux

CVE-2022-33637 | Important | Tampering | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Defender for Endpoint for Linux.

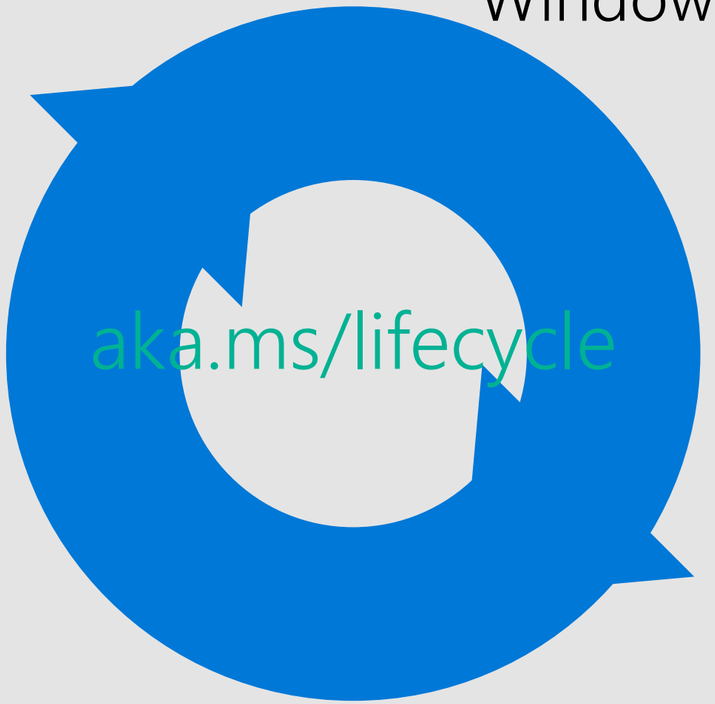
Product Lifecycle Update

Products reaching EoS in July

SQL Server 2012
System Center 2012
System Center 2012 R2

Windows 10 Semi-Annual Channel end of service – nothing in July

Windows Server, v20H2 EoS August



SQL Server 2012 and Windows Server 2012/2012 R2 end of support

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5016264	July 2022
Windows Server 2012	5016263	July 2022
Windows 10 1607/Server 2016	5016058	July 2022
Windows 10 1809/Server 2019	5005112	August 2021
Windows 10 20H2/Windows Server, version 20H2	5005260	August 2021
Windows 10 21H1	5005260	August 2021

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-21845	No	No	Kernel
CVE-2022-22711	No	No	BitLocker
CVE-2022-30202	No	No	Advanced Local Procedure Call
CVE-2022-30203	No	No	Boot Manager
CVE-2022-30205	No	No	Group Policy
CVE-2022-30206	No	No	Print Spooler
CVE-2022-30208	No	No	SAM
CVE-2022-30209	No	No	IIS Server
CVE-2022-30211	No	No	L2TP
CVE-2022-30212	No	No	Connected Devices Platform Service
CVE-2022-30213	No	No	GDI+
CVE-2022-30214	No	No	DNS Server
CVE-2022-30215	No	No	ADFS
CVE-2022-30216	No	No	Server Service

CVE	Public	Exploited	Product
CVE-2022-30220	No	No	Common Log File System Driver
CVE-2022-30221	No	No	Graphics Component
CVE-2022-30222	No	No	Shell
CVE-2022-30223	No	No	Hyper-V
CVE-2022-30224	No	No	Advanced Local Procedure Call
CVE-2022-30225	No	No	Media Player Network Sharing Service
CVE-2022-30226	No	No	Print Spooler
CVE-2022-22022	No	No	Print Spooler
CVE-2022-22023	No	No	Portable Device Enumerator Service
CVE-2022-22024	No	No	Fax Service
CVE-2022-22025	No	No	Internet Information Services Cachuri Module
CVE-2022-22026	No	No	CSRSS
CVE-2022-22027	No	No	Fax Service
CVE-2022-22028	No	No	Network File System

CVE	Public	Exploited	Product
CVE-2022-22029	No	No	Network File System
CVE-2022-22031	No	No	Credential Guard Domain-joined Public Key
CVE-2022-22034	No	No	Graphics Component
CVE-2022-22036	No	No	Performance Counters for
CVE-2022-22037	No	No	Advanced Local Procedure Call
CVE-2022-22038	No	No	Remote Procedure Call Runtime
CVE-2022-22039	No	No	Network File System
CVE-2022-22040	No	No	Internet Information Services Dynamic Compression Module
CVE-2022-22041	No	No	Print Spooler
CVE-2022-22042	No	No	Hyper-V
CVE-2022-22043	No	No	Fast FAT File System Driver
CVE-2022-22045	No	No	.Devices.Picker.dll
CVE-2022-22047	No	Yes	CSRSS
CVE-2022-22048	No	No	BitLocker

CVE	Public	Exploited	Product
CVE-2022-22049	No	No	CSRSS
CVE-2022-22050	No	No	Fax Service
CVE-2022-33632	No	No	Office
CVE-2022-33633	No	No	Skype for Business and Lync
CVE-2022-30181	No	No	Azure Site Recovery
CVE-2022-33637	No	No	Defender for Endpoint
CVE-2022-33641	No	No	Azure Site Recovery
CVE-2022-33642	No	No	Azure Site Recovery
CVE-2022-33643	No	No	Azure Site Recovery
CVE-2022-30187	No	No	Azure Storage Library

CVE	Public	Exploited	Product
CVE-2022-33644	No	No	Xbox Live Save Service
CVE-2022-33650	No	No	Azure Site Recovery
CVE-2022-23816	No	No	AMD: CVE-2022-23816 AMD CPU Branch Type Confusion
CVE-2022-33651	No	No	Azure Site Recovery
CVE-2022-33652	No	No	Azure Site Recovery
CVE-2022-33653	No	No	Azure Site Recovery
CVE-2022-33654	No	No	Azure Site Recovery
CVE-2022-33655	No	No	Azure Site Recovery
CVE-2022-33656	No	No	Azure Site Recovery
CVE-2022-33657	No	No	Azure Site Recovery
CVE-2022-33658	No	No	Azure Site Recovery
CVE-2022-33659	No	No	Azure Site Recovery
CVE-2022-33660	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-33661	No	No	Azure Site Recovery
CVE-2022-33662	No	No	Azure Site Recovery
CVE-2022-33663	No	No	Azure Site Recovery
CVE-2022-33664	No	No	Azure Site Recovery
CVE-2022-33665	No	No	Azure Site Recovery
CVE-2022-33666	No	No	Azure Site Recovery
CVE-2022-33667	No	No	Azure Site Recovery
CVE-2022-33668	No	No	Azure Site Recovery
CVE-2022-33669	No	No	Azure Site Recovery
CVE-2022-33671	No	No	Azure Site Recovery
CVE-2022-33672	No	No	Azure Site Recovery
CVE-2022-23825	No	No	AMD: CVE-2022-23825 AMD CPU Branch Type Confusion
CVE-2022-33673	No	No	Azure Site Recovery
CVE-2022-33674	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-33675	No	No	Azure Site Recovery
CVE-2022-33676	No	No	Azure Site Recovery
CVE-2022-33677	No	No	Azure Site Recovery
CVE-2022-33678	No	No	Azure Site Recovery