Microsoft

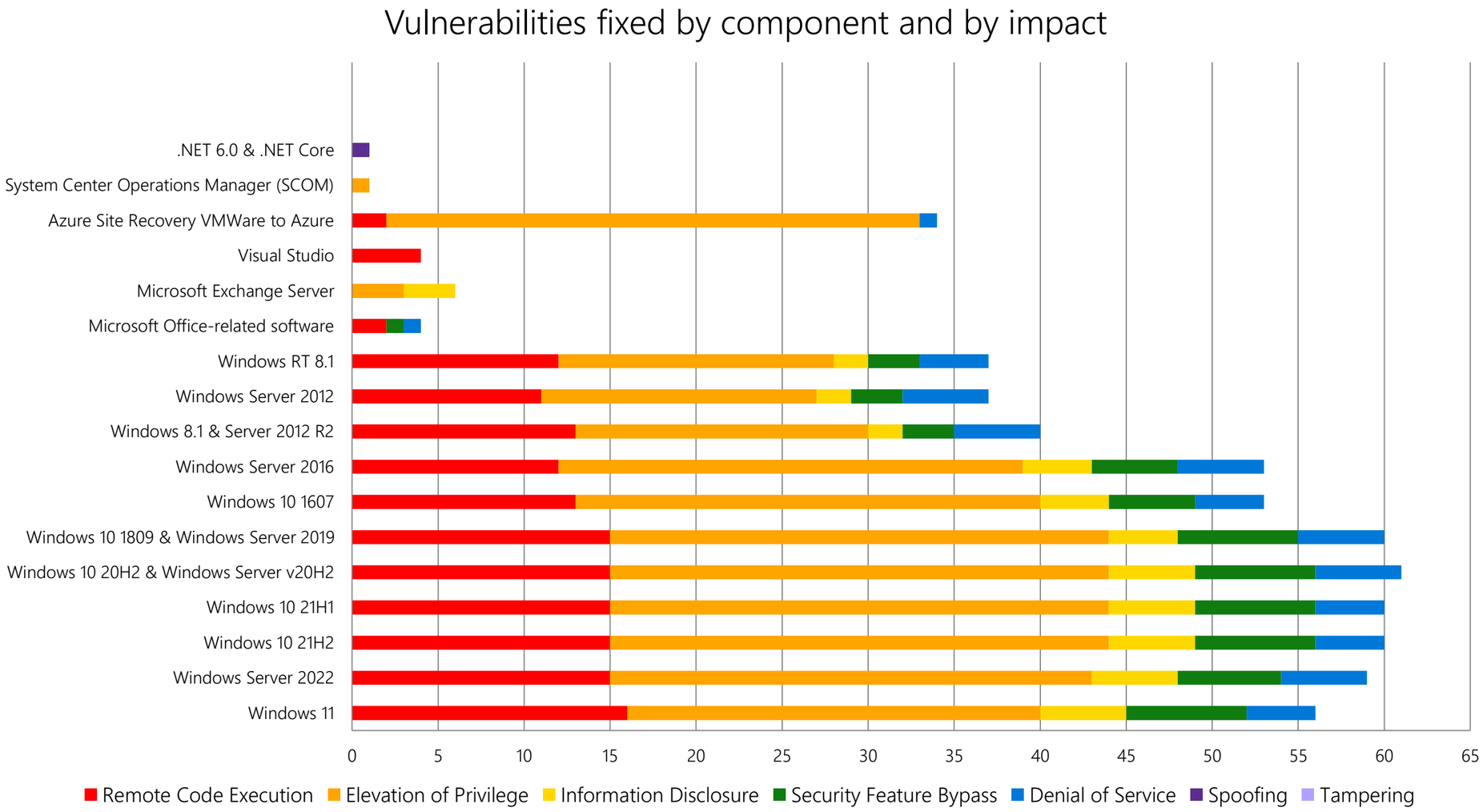
Microsoft Security Release

August 9, 2022

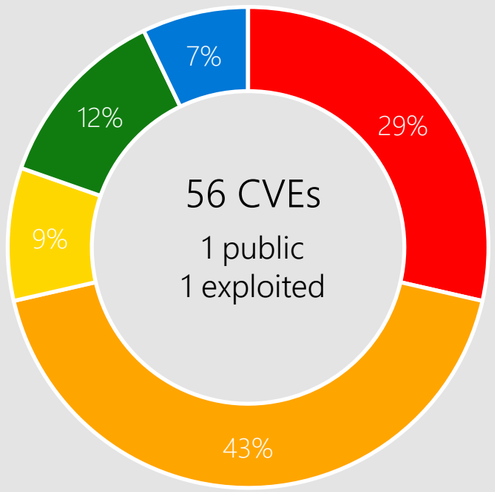
Agenda

- Security Updates
- Security Advisory
- Product Support Lifecycle
- Other resources related to the release

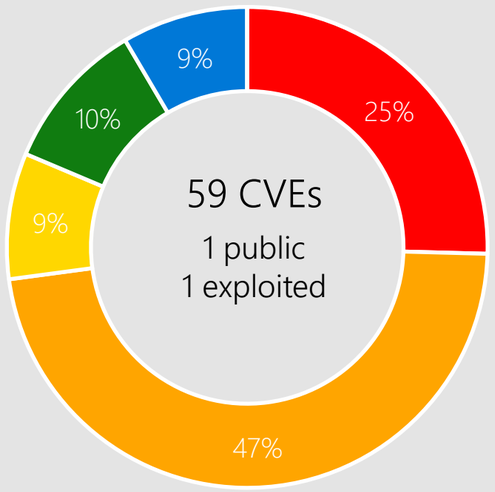
Monthly Security Release Overview - August 2022



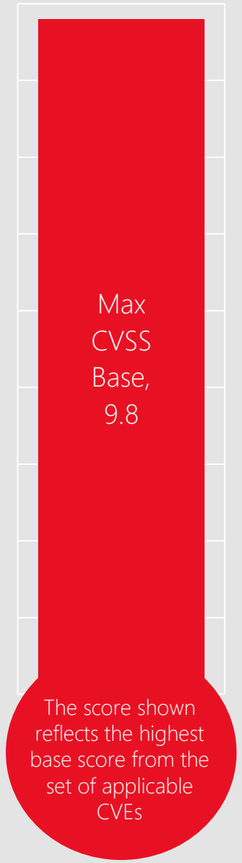
Windows 11, Server 2022



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-2022-34715 Network File System

Impact, Severity, Disclosure

Remote Code Execution | Important | 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

This vulnerability is not exploitable in NFSV2.0 or NFSV3.0.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022

CVE-2022-30133 Point-to-Point Protocol (PPP)

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

This vulnerability can only be exploited by communicating via Port 1723. As a temporary workaround prior to installing the updates that address this vulnerability, you can block traffic through that port thus rendering the vulnerability unexploitable.
Disabling Port 1723 could affect communications over your network.

Affected Software

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

CVE-2022-35804 SMB Client and Server

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.

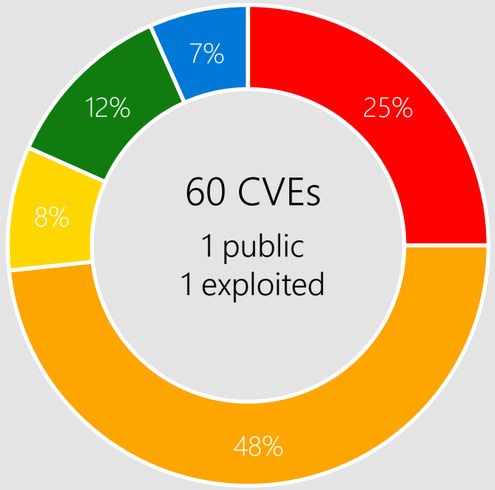
Workarounds

Disable SMBv3 compression. See CVE entry for details.

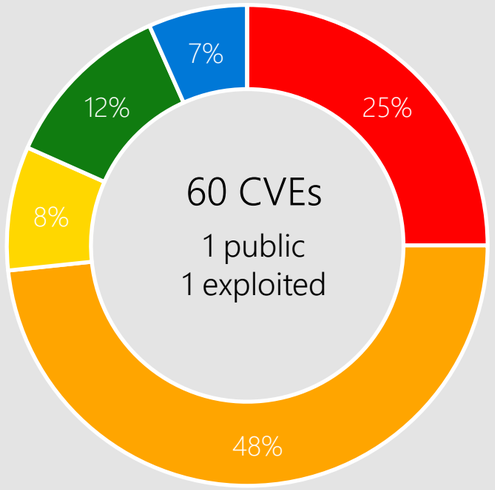
Affected Software

Windows 11

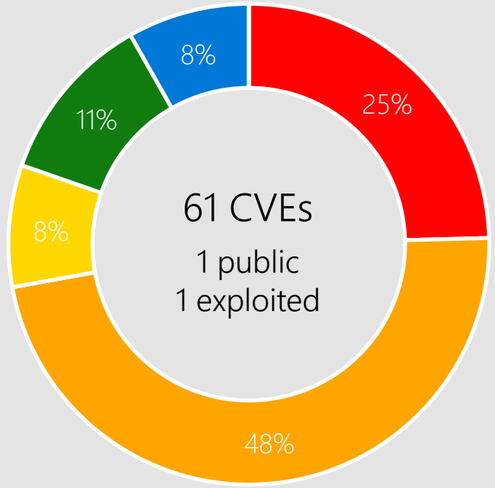
Windows 10



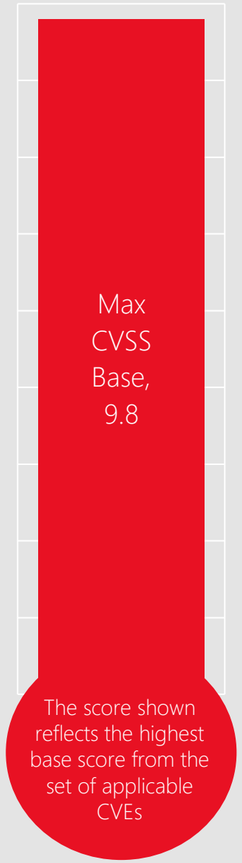
Windows 10 21H2



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-2022-34691 AD Domain Services

Impact, Severity, Disclosure

Elevation of Privilege | Critical | 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

A system is vulnerable only if Active Directory Certificate Services is running on the domain.

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-2022-34713 Support Diagnostic Tool (MSDT)

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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.

More Information

In May, Microsoft released a blog giving guidance for a vulnerability in MSDT and released updates to address it shortly thereafter. Public discussion of a vulnerability can encourage further scrutiny on the component, both by Microsoft security personnel as well as our research partners. This CVE is a variant of the vulnerability publicly known as Dogwalk.

Affected Software

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

CVE-2022-35797 Windows Hello

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 6.1 | Attack Vector: Physical | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

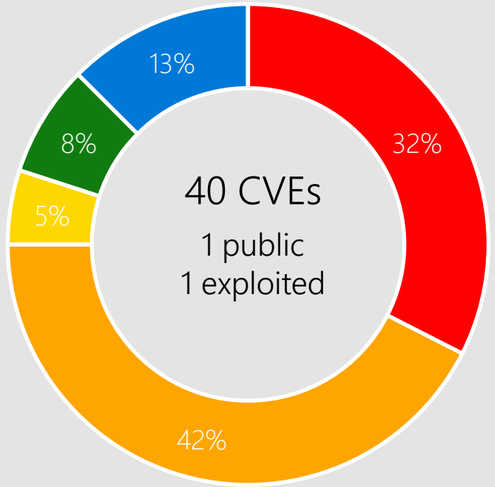
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

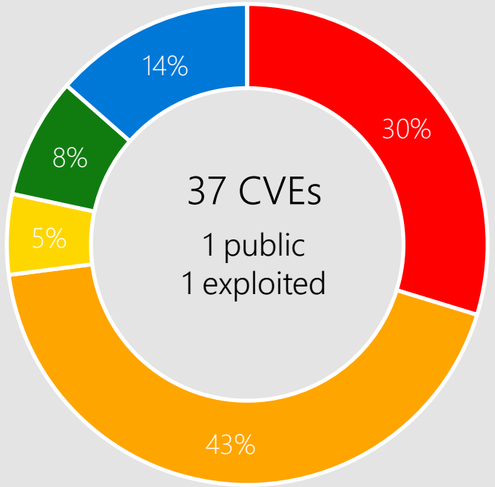
Affected Software

Windows 11
Windows 10

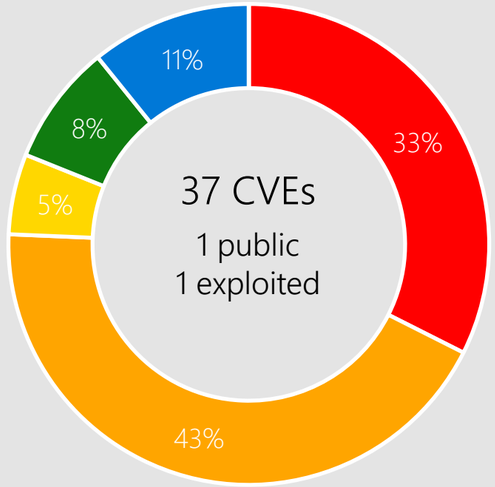
Windows 8.1, Server 2012 R2, and Server 2012



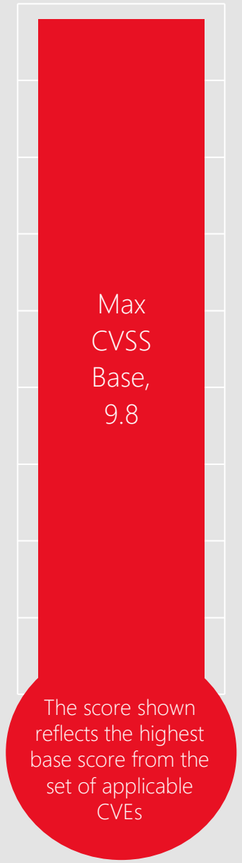
Windows 8.1 & Server 2012 R2



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-2022-34714 Secure Socket Tunneling Protocol (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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-34696 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

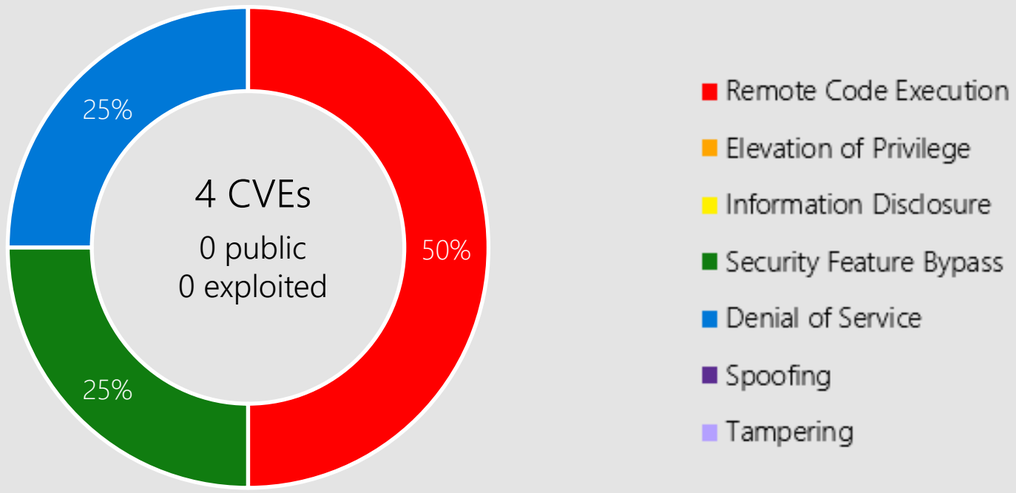
Workarounds

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
- Windows 8.1

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Outlook 2013/2016
Excel 2013/2016
365 Apps Enterprise
Office LTSC 2021
Office Online Server

CVE-2022-34717 Office

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

Office 2016
Office 2013
Office LTSC 2021
Office 2019
365 Apps Enterprise

Other Products

Exchange Server

CVE-2022-24477/21980/24516 | Critical | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22.

CVE-2022-30134 | Important | Information Disclosure | Public: Yes | Exploited: No

CVSS Base Score 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11.

Other Products

Exchange Server

CVE-2022-21979 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 4.8
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23.

CVE-2022-34692 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

Other Products

.NET Core and .NET 6.0

CVE-2022-34716 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.9
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET Core 3.1, .NET 6.0.

Other Products

Visual Studio

CVE-2022-35777/35825/35826/35827 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2013 Update 5, Visual Studio 2012 Update 5, Visual Studio 2022 version 17.2, 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 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Azure Site Recovery VMWare to Azure

CVE-2022-35802 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure Site Recovery VMWare to Azure.

CVE-2022-35772/35824 | 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-2022-35775/35780-35782/35784-35786/35788-35791/35799/35801/35807-35811/35813-35819 | 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-2022-35776 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 6.2
Attack Vector: Adjacent
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-2022-35774/35787/35800 | 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.

CVE-2022-35783/35812 | 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

System Center Operations Manager

CVE-2022-33640 | 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: System Center Operations Manager (SCOM) 2019, System Center Operations Manager (SCOM) 2016, System Center Operations Manager (SCOM) 2022.

Other Products

Open Management Infrastructure

CVE-2022-33640 | 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: Open Management Infrastructure

Other Products

Azure

CVE-2022-33646 Azure Batch
CVE-2022-35821 Azure Sphere
CVE-2022-30175/30176/34685/34686/34687/35773/35779/35806 Azure RTOS GUIX

Security Advisory Re-Release ADV200011

What's Changed?

Microsoft has released standalone security update 5012170 to address the Secure Boot DBX vulnerabilities described in this advisory.

Suggested Actions:

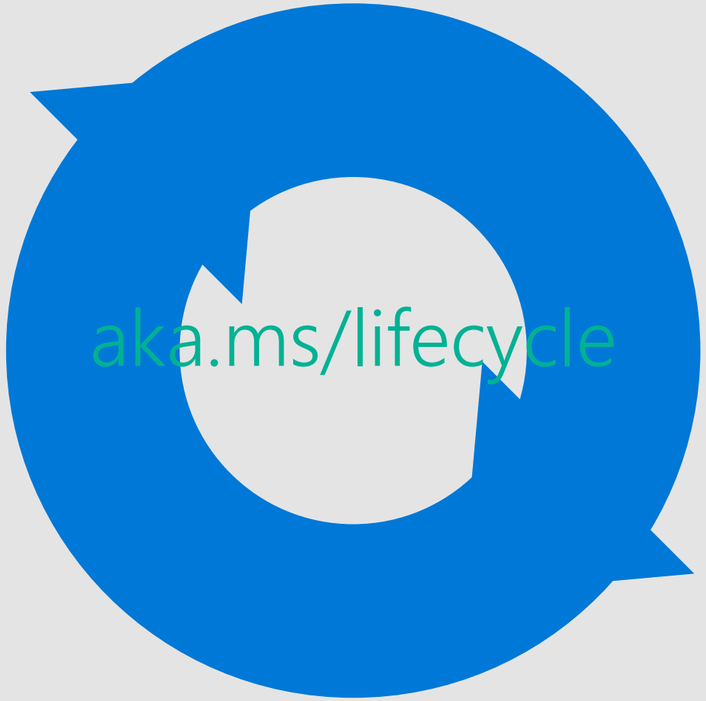
1. Install standalone security update 5012170
2. If you cannot apply update immediately, apply mitigations listed in advisory.

ADV200011 - Security Update Guide - Microsoft - Microsoft Guidance for Addressing Security Feature Bypass in GRUB

Product Lifecycle Update

Windows 10 Semi-Annual Channel
end of service

Windows Server 20H2



Latest Servicing Stack Updates

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-30133	No	No	Point-to-Point Protocol (PPP)
CVE-2022-30144	No	No	Bluetooth Service
CVE-2022-30194	No	No	WebBrowser Control
CVE-2022-30197	No	No	Kernel
CVE-2022-33670	No	No	Partition Management Driver
CVE-2022-34696	No	No	Hyper-V
CVE-2022-34699	No	No	Win32k
CVE-2022-34703	No	No	Partition Management Driver
CVE-2022-34706	No	No	Local Security Authority (LSA)
CVE-2022-34707	No	No	Kernel
CVE-2022-34708	No	No	Kernel
CVE-2022-34709	No	No	Defender Credential Guard
CVE-2022-34710	No	No	Defender Credential Guard

CVE	Public	Exploited	Product
CVE-2022-34712	No	No	Defender Credential Guard
CVE-2022-34713	Yes	Yes	Support Diagnostic Tool (MSDT)
CVE-2022-34714	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-34715	No	No	Network File System
CVE-2022-35743	No	No	Support Diagnostic Tool (MSDT)
CVE-2022-35744	No	No	Point-to-Point Protocol (PPP)
CVE-2022-35745	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-35746	No	No	Digital Media Receiver
CVE-2022-35747	No	No	Point-to-Point Protocol (PPP)
CVE-2022-35748	No	No	HTTP.sys
CVE-2022-35749	No	No	Digital Media Receiver
CVE-2022-35750	No	No	Win32k
CVE-2022-35751	No	No	Hyper-V
CVE-2022-35754	No	No	Unified Write Filter

CVE	Public	Exploited	Product
CVE-2022-35755	No	No	Print Spooler
CVE-2022-35756	No	No	Kerberos
CVE-2022-35757	No	No	Cloud Files Mini Filter Driver
CVE-2022-35758	No	No	Kernel Memory
CVE-2022-35759	No	No	Local Security Authority (LSA)
CVE-2022-35761	No	No	Kernel
CVE-2022-35762	No	No	Storage Spaces Direct
CVE-2022-35763	No	No	Storage Spaces Direct
CVE-2022-35764	No	No	Storage Spaces Direct
CVE-2022-35765	No	No	Storage Spaces Direct
CVE-2022-35792	No	No	Storage Spaces Direct
CVE-2022-34303	No	No	CERT/CC: CVE-20220-34303 Crypto Pro Boot Loader Bypass
CVE-2022-34301	No	No	CERT/CC: CVE-2022-34301 Eurosoft Boot Loader Bypass
CVE-2022-35804	No	No	SMB Client and Server

CVE	Public	Exploited	Product
CVE-2022-34302	No	No	CERT/CC: CVE-2022-34302 New Horizon Data Systems Inc Boot Loader Bypass
CVE-2022-34690	No	No	Fax Service
CVE-2022-34701	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-34702	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-34704	No	No	Defender Credential Guard
CVE-2022-34705	No	No	Defender Credential Guard
CVE-2022-35766	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-35767	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-35793	No	No	Print Spooler
CVE-2022-35768	No	No	Kernel
CVE-2022-35795	No	No	Error Reporting Service
CVE-2022-35771	No	No	Defender Credential Guard

CVE	Public	Exploited	Product
CVE-2022-35797	No	No	Hello
CVE-2022-35820	No	No	Bluetooth Driver
CVE-2022-35794	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-35769	No	No	Point-to-Point Protocol (PPP)

CVE	Public	Exploited	Product
CVE-2022-34717	No	No	Office
CVE-2022-30175	No	No	Azure RTOS GUIX Studio
CVE-2022-30176	No	No	Azure RTOS GUIX Studio
CVE-2022-33640	No	No	System Center Operations Manager: Open Management Infrastructure (OMI)
CVE-2022-33646	No	No	Azure Batch Node Agent
CVE-2022-34685	No	No	Azure RTOS GUIX Studio
CVE-2022-34686	No	No	Azure RTOS GUIX Studio
CVE-2022-34687	No	No	Azure RTOS GUIX Studio
CVE-2022-34691	No	No	Active Directory Domain Services
CVE-2022-35760	No	No	ATA Port Driver
CVE-2022-35773	No	No	Azure RTOS GUIX Studio
CVE-2022-35776	No	No	Azure Site Recovery
CVE-2022-35802	No	No	Azure Site Recovery
CVE-2022-35780	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-35781	No	No	Azure Site Recovery
CVE-2022-21979	No	No	Exchange
CVE-2022-21980	No	No	Exchange Server
CVE-2022-24516	No	No	Exchange Server
CVE-2022-24477	No	No	Exchange Server
CVE-2022-30134	Yes	No	Exchange Server
CVE-2022-34692	No	No	Exchange
CVE-2022-34716	No	No	.NET
CVE-2022-35772	No	No	Azure Site Recovery
CVE-2022-35799	No	No	Azure Site Recovery
CVE-2022-35774	No	No	Azure Site Recovery
CVE-2022-35800	No	No	Azure Site Recovery
CVE-2022-35775	No	No	Azure Site Recovery
CVE-2022-35801	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-35777	No	No	Visual Studio
CVE-2022-35779	No	No	Azure RTOS GUIX Studio
CVE-2022-35806	No	No	Azure RTOS GUIX Studio
CVE-2022-35807	No	No	Azure Site Recovery
CVE-2022-35808	No	No	Azure Site Recovery
CVE-2022-35782	No	No	Azure Site Recovery
CVE-2022-35809	No	No	Azure Site Recovery
CVE-2022-35783	No	No	Azure Site Recovery
CVE-2022-35784	No	No	Azure Site Recovery
CVE-2022-35810	No	No	Azure Site Recovery
CVE-2022-35811	No	No	Azure Site Recovery
CVE-2022-35785	No	No	Azure Site Recovery
CVE-2022-35812	No	No	Azure Site Recovery
CVE-2022-35786	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-35787	No	No	Azure Site Recovery
CVE-2022-35813	No	No	Azure Site Recovery
CVE-2022-35788	No	No	Azure Site Recovery
CVE-2022-35814	No	No	Azure Site Recovery
CVE-2022-35789	No	No	Azure Site Recovery
CVE-2022-35815	No	No	Azure Site Recovery
CVE-2022-35790	No	No	Azure Site Recovery
CVE-2022-35816	No	No	Azure Site Recovery
CVE-2022-35817	No	No	Azure Site Recovery
CVE-2022-35791	No	No	Azure Site Recovery
CVE-2022-35818	No	No	Azure Site Recovery
CVE-2022-35819	No	No	Azure Site Recovery
CVE-2022-35821	No	No	Azure Sphere
CVE-2022-35824	No	No	Azure Site Recovery

CVE	Public	Exploited	Product
CVE-2022-35825	No	No	Visual Studio
CVE-2022-35826	No	No	Visual Studio
CVE-2022-35827	No	No	Visual Studio