Microsoft

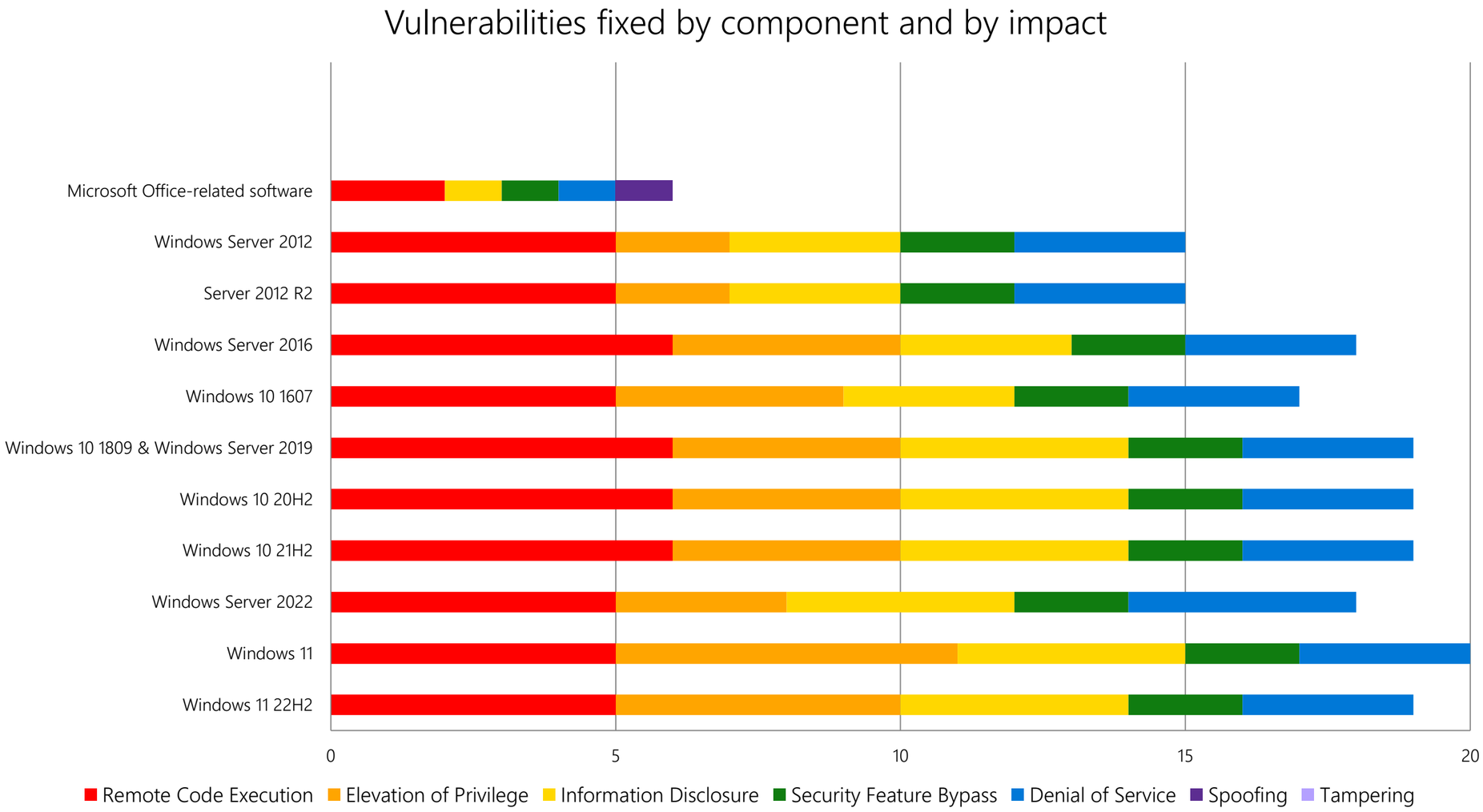
Microsoft Security Release

May 9, 2023

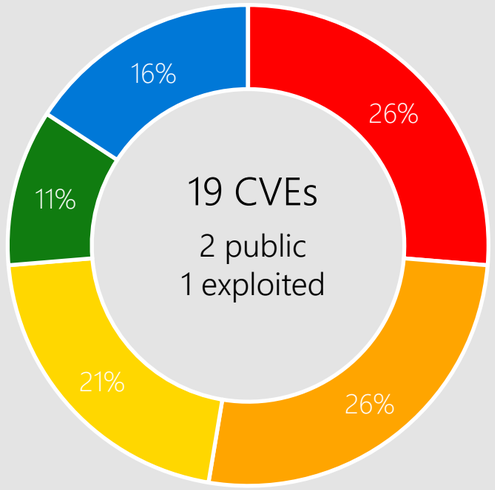
Agenda

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

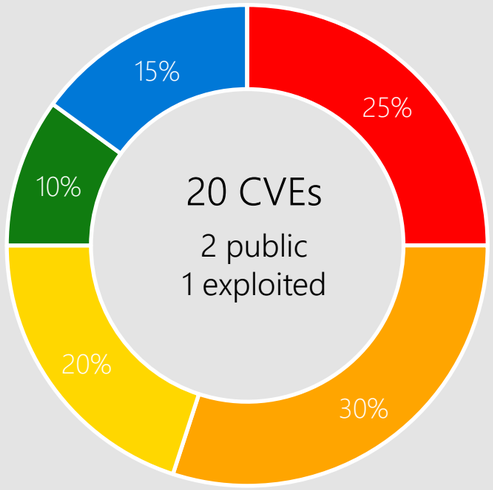
Monthly Security Release Overview - May 2023



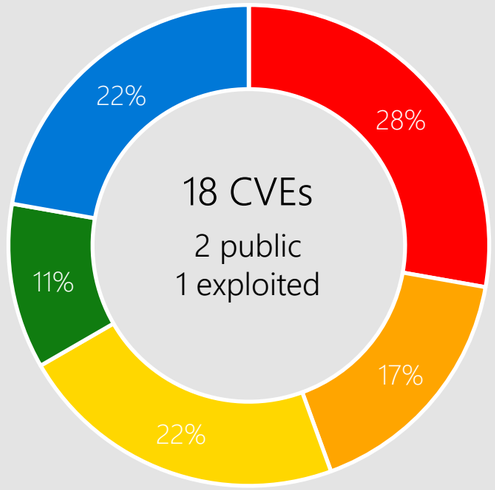
Windows 11, Server 2022



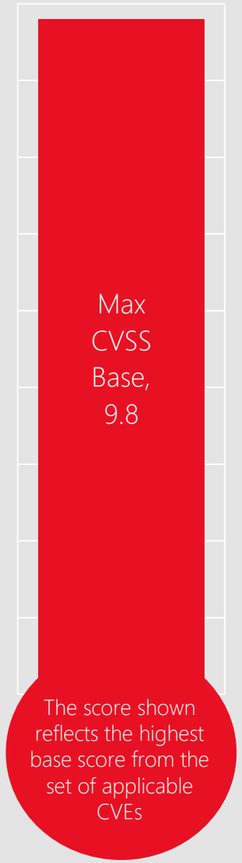
Windows 11 22H2



Windows 11



Windows Server 2022



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

Affected Components:

Backup Service
Bluetooth Driver
Driver Revocation List
Graphics Component
iSCSI Target Service
Kernel
Lightweight Directory Access Protocol (LDAP)
MSHTML Platform
NFS Portmapper
NTLM Security Support Provider
OLE
Pragmatic General Multicast (PGM)
Remote Desktop Client
Remote Procedure Call Runtime
Secure Boot
Secure Socket Tunneling Protocol (SSTP)
Server for NFS
Win32k

CVE-2023-24943 Pragmatic General Multicast (PGM)

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

Only PGM Server is vulnerable to this vulnerability. To mitigate risk, Microsoft recommends customers deploy newer technologies such as Unicast or Multicast server.

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

CVE-2023-24941 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

This vulnerability is not exploitable in NFSV2.0 or NFSV3.0. Please see CVE entry for details on disabling NFS v4.1 and important precautions.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-24932 Secure Boot

Impact, Severity, Disclosure

Security Feature Bypass| Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 6.7 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: High | User Interaction: None

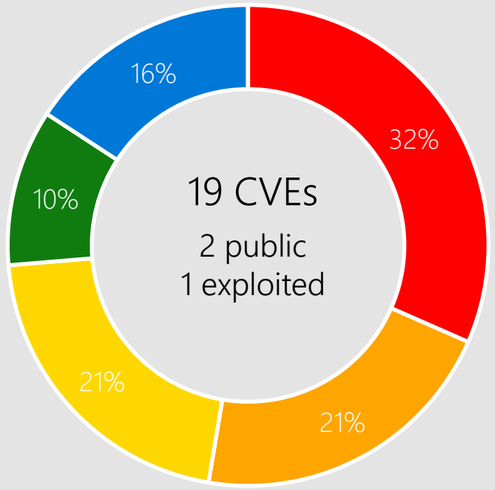
More Information

Read MSRC blog for overview: Microsoft Security Response Center
Read KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 to learn about the phased deployment, additional actions necessary for complete protection, and potential impact

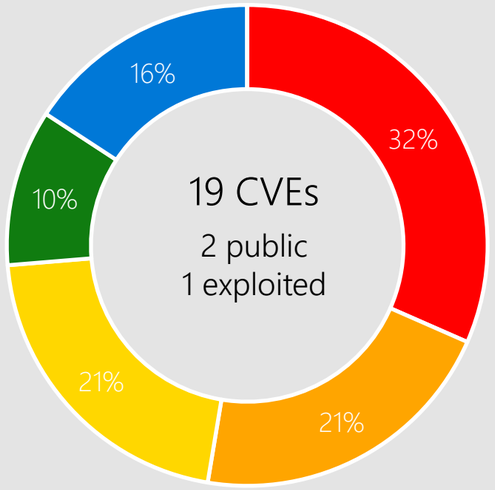
Affected Software

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

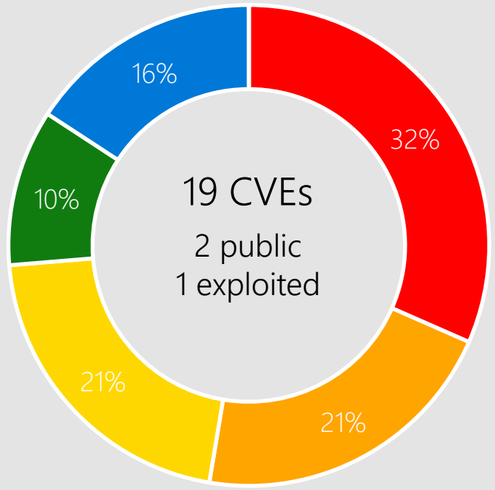
Windows 10



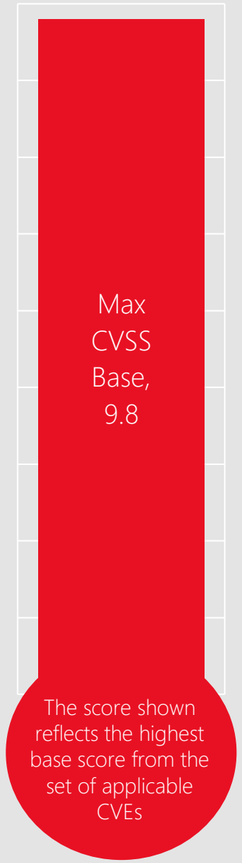
Windows 10 22H2



Windows 10 21H2



Windows 10 20H2



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:

Backup Service
Bluetooth Driver
Driver Revocation List

iSCSI Target Service
Kernel
Lightweight Directory Access Protocol (LDAP)

MSHTML Platform
Network File System
NFS Portmapper

NTLM Security Support Provider
OLE
Pragmatic General Multicast (PGM)

Remote Procedure Call Runtime
Secure Boot
Secure Socket Tunneling Protocol (SSTP)

CVE-2023-29325 OLE

Impact, Severity, Disclosure

Remote Code Execution | Critical | Publicly 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

Read email messages in plain text format. See CVE entry for details.

Affected Software

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

CVE-2023-29336 Win32k

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 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-24947 Bluetooth Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

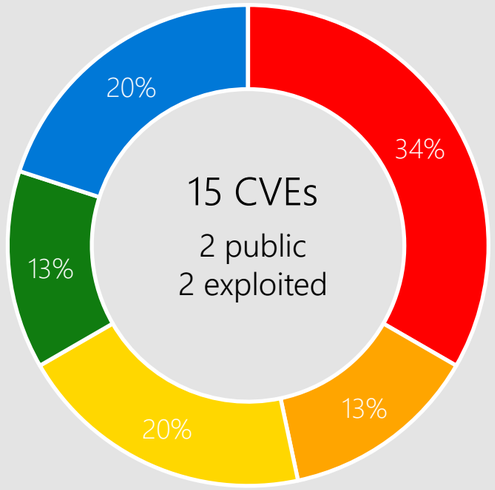
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

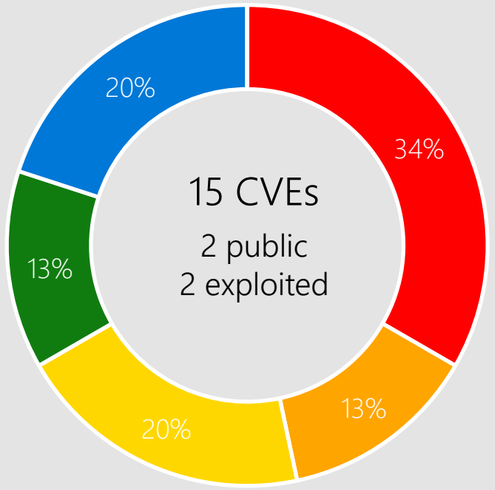
Affected Software

Server 2019
Windows 10
Server 2016

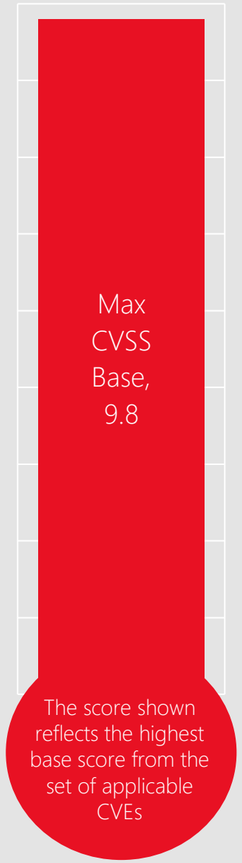
Server 2012 R2, and Server 2012



Windows 8.1 & Server 2012 R2



Windows Server 2012



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

Affected Components:

Bluetooth Driver
Driver Revocation List
iSCSI Target Service

Lightweight Directory Access Protocol (LDAP)
Network File System
NFS Portmapper

NTLM Security Support Provider
OLE
Pragmatic General Multicast (PGM)

Remote Procedure Call Runtime
Secure Boot
Secure Socket Tunneling Protocol (SSTP)

CVE-2023-28283 LDAP

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

CVE-2023-24903 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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-29324 MSHTML Platform

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 6.5 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

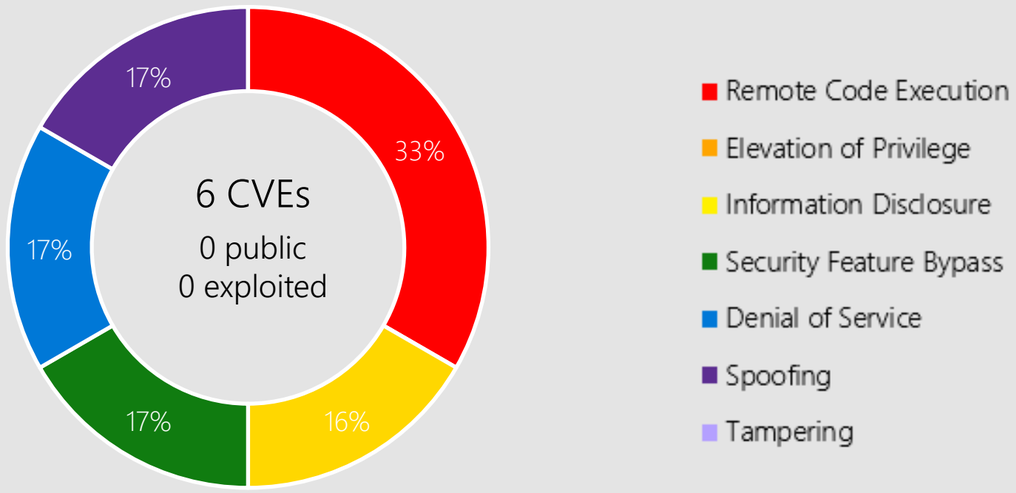
More Information

[Microsoft Mitigates Outlook Elevation of Privilege Vulnerability | MSRC Blog | Microsoft Security Response Center]

Affected Software

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

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
Word 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
SharePoint Server Subscription Edition
Teams

CVE-2023-24953 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 LTSC 2021
Office LTSC for Mac 2021
Excel 2013
Excel 2016
Office 2019 for Mac
Office 2019
365 Apps Enterprise
Office Online Server

Other Products

Visual Studio

CVE-2023-29338 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio Code.

Other Products

Windows Sysmon

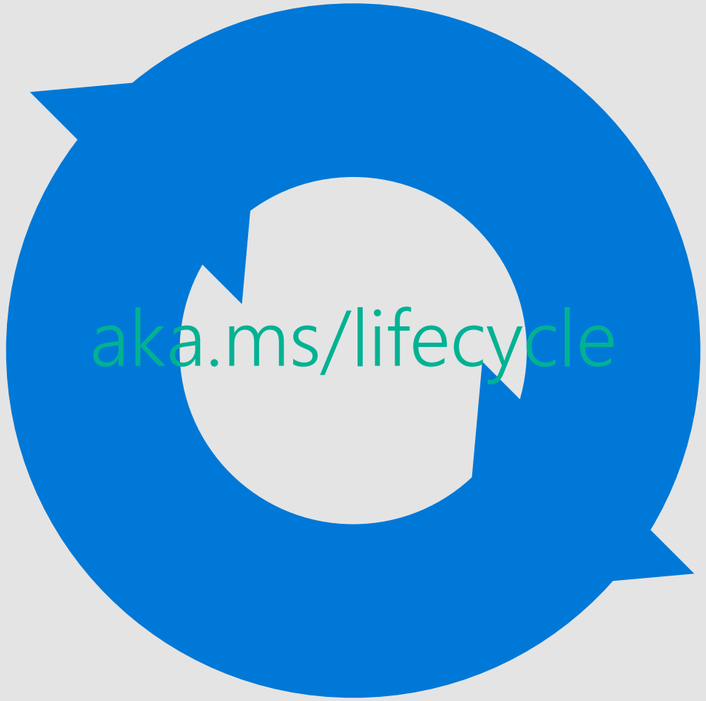
CVE-2023-29343 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Windows Sysmon.

Product Lifecycle Update

Products reaching end of servicing

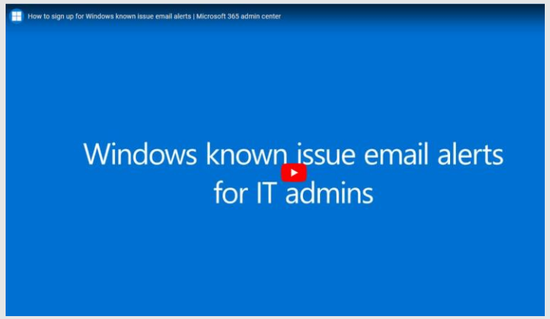
Windows 10, version 20H2



ADV990001 - Security Update Guide - Microsoft - Latest Servicing Stack Updates

New feature: Sign up for Windows known issue email alerts

- You can get notified about Windows known issues documented in the Windows release health section of the Microsoft 365 admin center.
- This enables you to easily and quickly learn about issues related to Windows updates and make informed decisions about rolling out an update across your environment.
- When you sign up, you'll receive emails about new issues for the versions of the Windows operating system you support, as well as updates to known issues such as:
  - Changes in issue status
  - New workarounds
  - Issue resolution
- This new feature is available to IT admins with a Windows or Microsoft 365 tenant, a subscription that provides access to Windows release health in the Microsoft 365 admin center[1], and an eligible admin role.
- Read more at: https://aka.ms/WRH/NotifyMe



Watch this short video for a quick step-by-step on how to set up email notifications for Windows known issues.

https://youtu.be/QSD7fYyodC4

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-28283	No	No	LDAP
CVE-2023-24898	No	No	SMB
CVE-2023-24899	No	No	Graphics Component
CVE-2023-24939	No	No	Server for NFS
CVE-2023-24900	No	No	NTLM Security Support Provider
CVE-2023-24940	No	No	PGM
CVE-2023-24901	No	No	NFS Portmapper
CVE-2023-24941	No	No	Network File System
CVE-2023-24902	No	No	Win32k
CVE-2023-24942	No	No	Remote Procedure Call Runtime
CVE-2023-24903	No	No	SSTP
CVE-2023-24943	No	No	PGM
CVE-2023-24944	No	No	Bluetooth Driver
CVE-2023-24945	No	No	iSCSI Target Service

CVE	Public	Exploited	Product
CVE-2023-24946	No	No	Backup Service
CVE-2023-24947	No	No	Bluetooth Driver
CVE-2023-24948	No	No	Bluetooth Driver
CVE-2023-24949	No	No	Kernel
CVE-2023-29324	No	No	MSHTML Platform
CVE-2023-29336	No	Yes	Win32k
CVE-2023-29340	No	No	AV1 Video Extension
CVE-2023-29341	No	No	AV1 Video Extension
CVE-2023-29343	No	No	SysInternals Sysmon for
CVE-2023-24932	Yes	Yes	Secure Boot
CVE-2023-28251	No	No	Driver Revocation List
CVE-2023-28290	No	No	Remote Desktop Protocol Client
CVE-2023-24904	No	No	Installer
CVE-2023-29325	Yes	No	OLE

CVE	Public	Exploited	Product
CVE-2023-24955	No	No	SharePoint Server
CVE-2023-29335	No	No	Word
CVE-2023-29333	No	No	Access
CVE-2023-29344	No	No	Office
CVE-2023-24881	No	No	Teams
CVE-2023-24905	No	No	Remote Desktop Client
CVE-2023-29338	No	No	Visual Studio Code