Microsoft

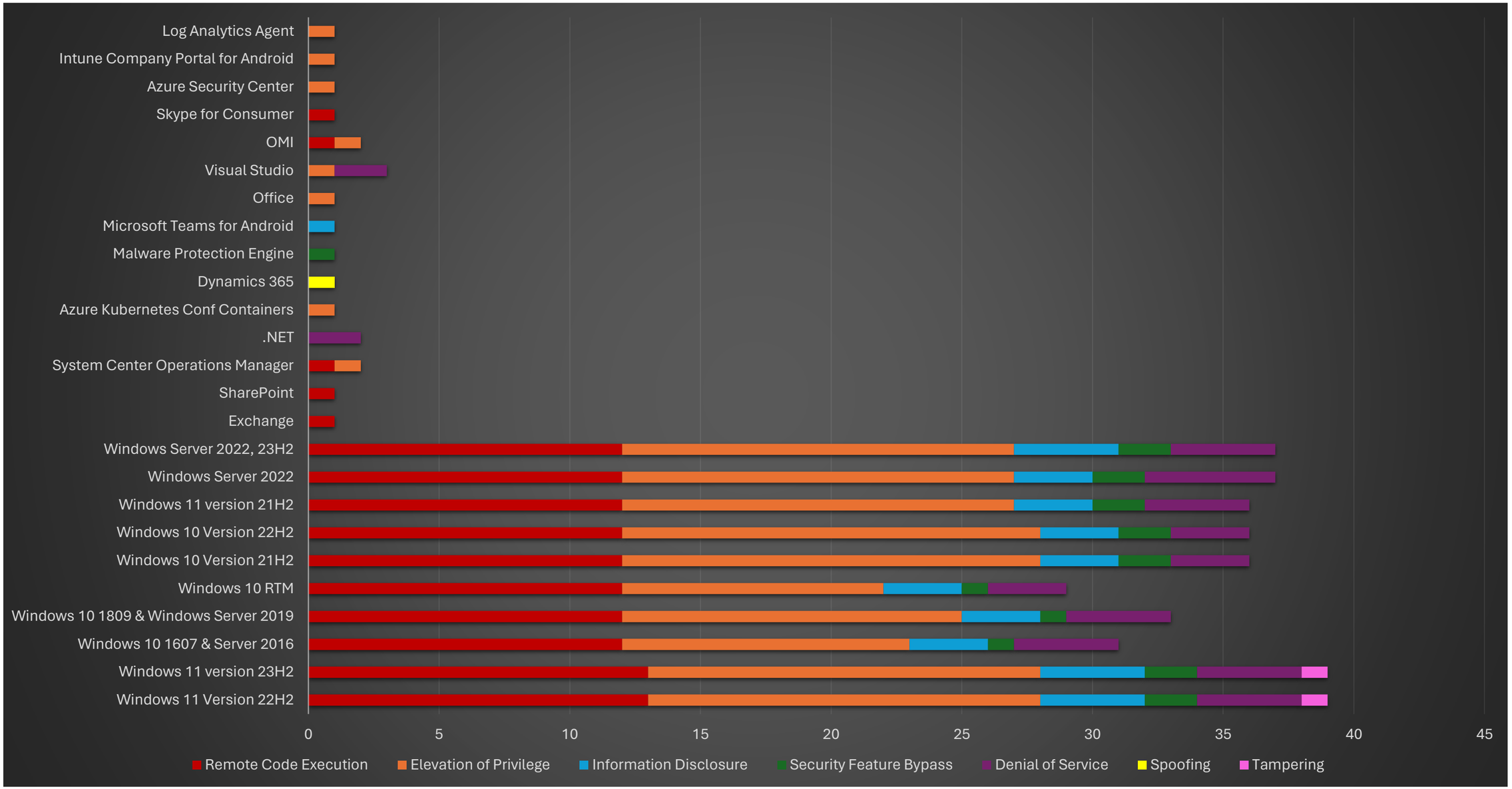
Microsoft Security Release

March 12, 2024

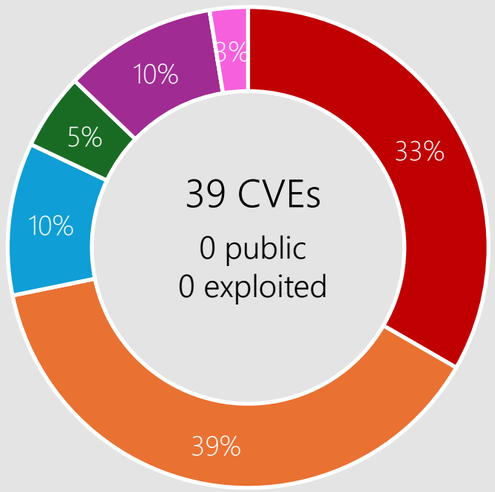
Agenda

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

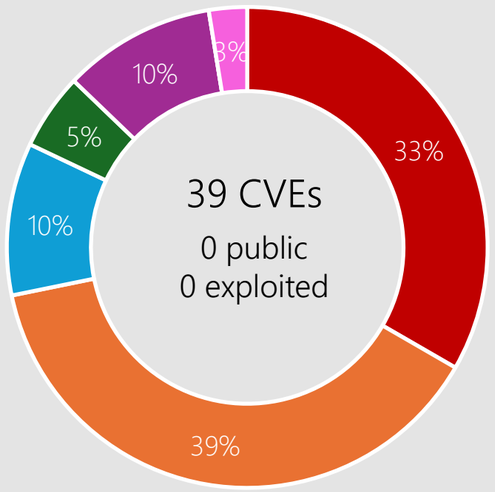
Microsoft Security Release Overview – March 2024



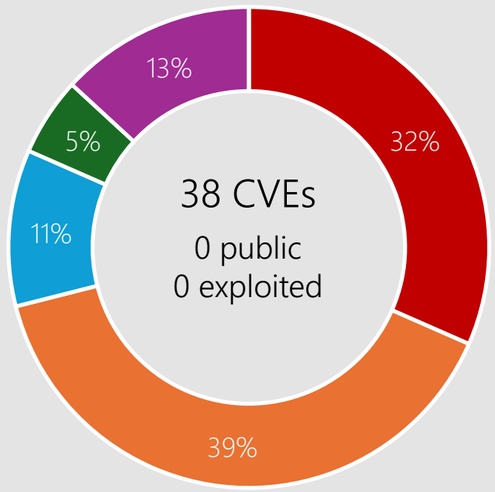
Windows 11, Server 2022



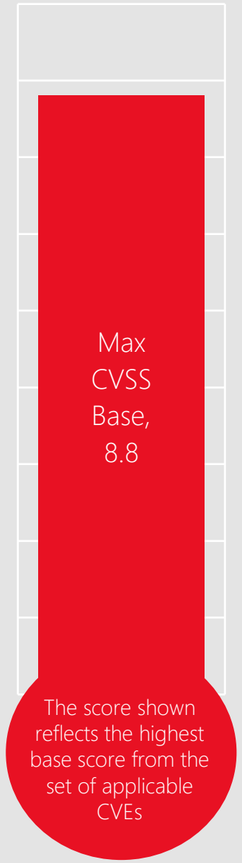
Windows 11 23H2



Windows 11 22H2



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-2024-21407 Hyper-V

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
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-21435 OLE

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.

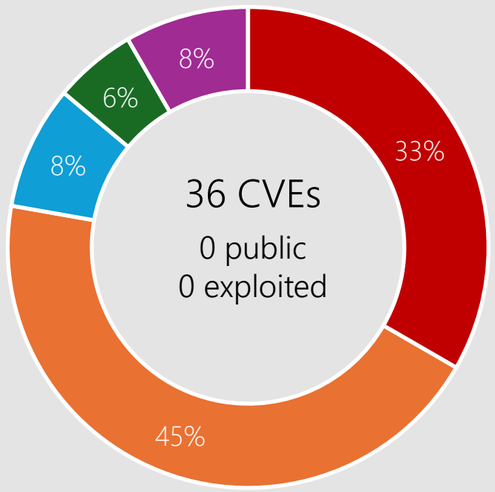
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

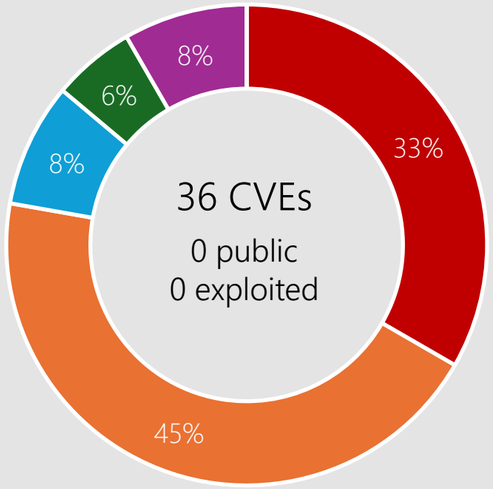
Affected Software

Windows 11

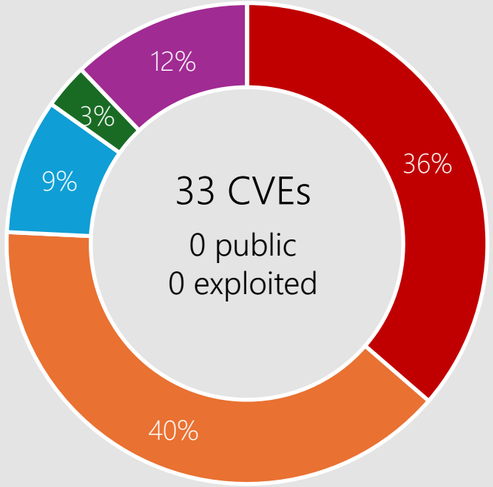
Windows 10



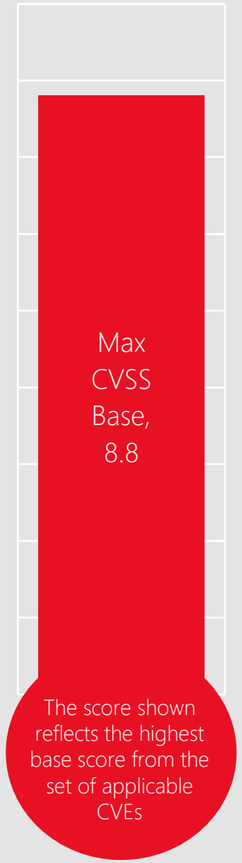
Windows 10 22H2



Windows 10 21H2



Windows 10 1809 & Windows Server 2019



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

Affected Components:

AllJoyn API
Composite Image File System (CimFS)
Error Reporting Service
Graphics Component
Hyper-V
HVCI
Installer
Kerberos
USB Hub Driver
Kernel
NTFS
ODBC Driver
Print Spooler
SCSI Class System File
Telephony Server
Update Stack
USB Attached SCSI (UAS) Protocol

CVE-2024-21441 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
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-21440 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.

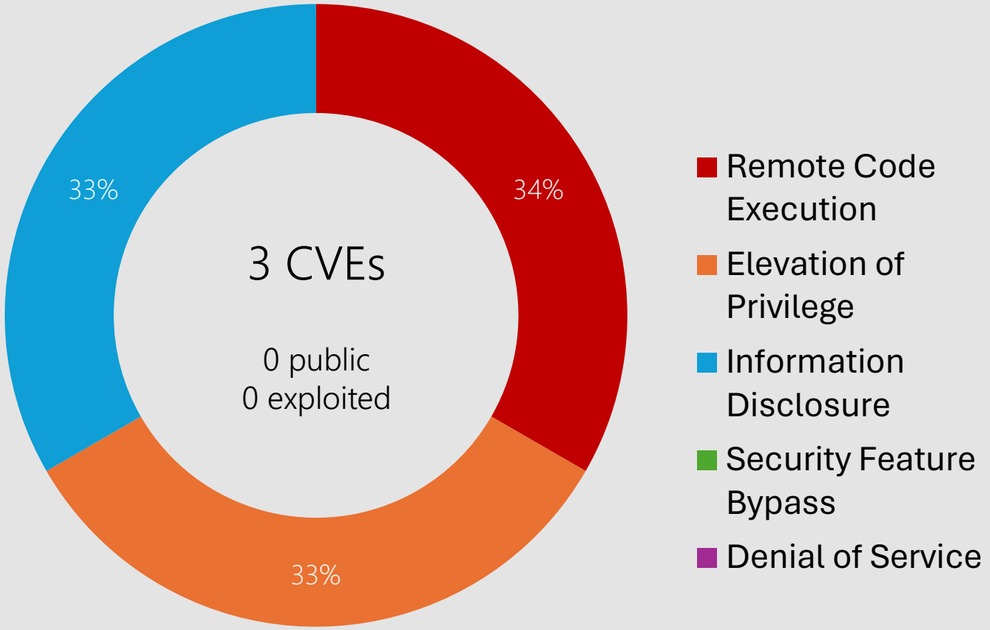
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
SharePoint Server Subscription Edition
Teams Android

CVE-2024-21426 SharePoint Server

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

SharePoint Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

CVE-2024-26199 Office

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | No known 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

365 Apps Enterprise

Other Products

Dynamics 365

CVE-2024-21419 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1.

Other Products

Exchange Server

CVE-2024-26198 | 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: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 13, Exchange Server 2019 Cumulative Update 14.

Other Products

System Center Operations Manager (SCOM) and OMI

CVE-2024-21334 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: System Center Operations Manager (SCOM) 2019, System Center Operations Manager (SCOM) 2022, Open Management Infrastructure

CVE-2024-21330 | 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) 2022, Open Management Infrastructure, Operations Management Suite Agent Linux (OMS).

Some Azure products that use OMS: Log Analytics Agent, Azure Security Center, Container Monitoring Solution, Azure Sentinel, Azure Automation, Azure Automation Update Management

Other Products

SQL Server

CVE-2024-26164 | Important | 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: SQL Server backend Django.

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-21392 | .NET and Visual Studio Denial of Service Vulnerability

Base CVSS: 7.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Visual Studio 2022, .NET 7.0, .NET 8.0

CVE-2024-26190 | Microsoft QUIC Denial of Service Vulnerability

Base CVSS: 7.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Visual Studio 2022, .NET 7.0, .NET 8.0, Windows 11, Windows Server 2022

Developer Tools

Visual Studio

CVE-2024-26165 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio Code.

Other Products

Azure Kubernetes Service Confidential Containers

CVE-2024-21400 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Azure Kubernetes Service Confidential Containers.

Other Products

Microsoft Authenticator

CVE-2024-21390 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Authenticator.

Other Products

Intune Company Portal for Android

CVE-2024-26201 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.6
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Intune Company Portal Android.

Other Products

Microsoft Outlook for Android

CVE-2024-26204 | 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: Outlook Android.

Other Products

Skype for Consumer

CVE-2024-21411 | 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: Skype Consumer.

Other Products

Windows Defender Antimalware Platform

CVE-2024-20671 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Windows Defender Antimalware Platm.

Other Products

Azure

CVE-2024-21418 Software for Open Networking in the Cloud (SONiC)
CVE-2024-26203 Azure Data Studio
CVE-2024-21421 Azure SDK

Advisory – Deprecation of Oracle’s libraries in Exchange Server

Summary

Microsoft is announcing the deprecation of the use of the Oracle Outside In libraries (also known as OutsideInModule or OIT) in Microsoft Exchange Server. This will be a three-phase deprecation process.

- The first phase will be to disable Oracle's Outside In Technology (OIT) for all file types.
- The second phase will introduce a modern in-house file scanning solution to replace Oracle's Outside In Technology, which was already blocked during the first phase.
- The third phase will completely remove the OIT code from Exchange Server.

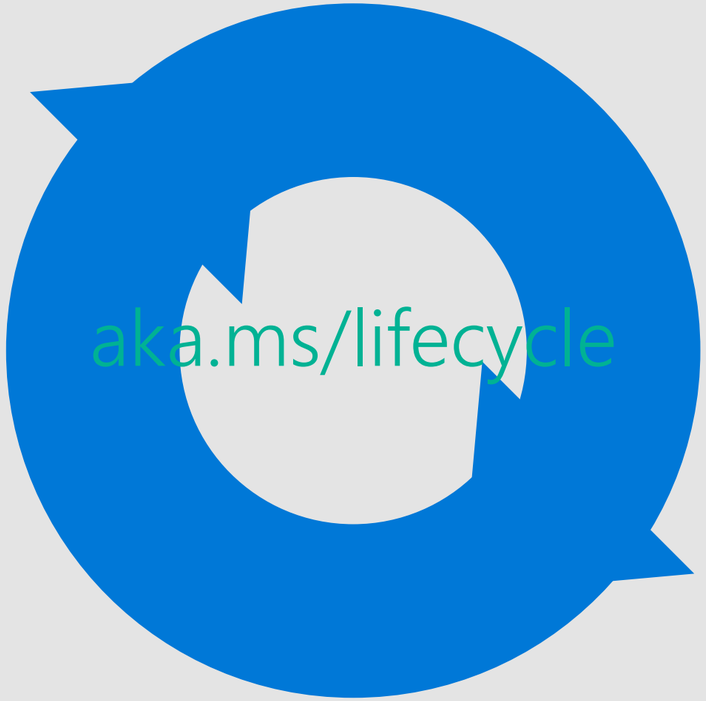
Recommended Actions:

Apply the March 2024 Exchange updates. This will update the OIT libraries, which addresses some of the known vulnerabilities documented here. This also prevents OIT from scanning any file types by default, and instead, alternative scanning modules are used.

https://msrc.microsoft.com/update-guide/advisory/ADV24199947

Product Lifecycle Update

No products reaching end of support
in March



Latest Servicing Stack Updates

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2024-20671	No	No	Defender
CVE-2024-21429	No	No	USB Hub Driver
CVE-2024-21430	No	No	USB Attached SCSI (UAS) Protocol
CVE-2024-21438	No	No	AllJoyn API
CVE-2024-21439	No	No	Telephony Server
CVE-2024-21442	No	No	USB Print Driver
CVE-2024-21443	No	No	Kernel
CVE-2024-21445	No	No	USB Print Driver
CVE-2024-21446	No	No	NTFS
CVE-2024-26197	No	No	Standards-Based Storage Management Service
CVE-2024-26159	No	No	ODBC Driver
CVE-2024-21407	No	No	Hyper-V
CVE-2024-21408	No	No	Hyper-V
CVE-2024-21427	No	No	Kerberos

CVE	Public	Exploited	Product
CVE-2024-21431	No	No	HVCI
CVE-2024-21432	No	No	Update Stack
CVE-2024-21433	No	No	Print Spooler
CVE-2024-21434	No	No	SCSI Class System File
CVE-2024-21435	No	No	OLE
CVE-2024-21436	No	No	Installer
CVE-2024-21437	No	No	Graphics Component
CVE-2024-21440	No	No	ODBC Driver
CVE-2024-26160	No	No	Cloud Files Mini Filter Driver
CVE-2024-26162	No	No	ODBC Driver
CVE-2024-26169	No	No	Error Reporting Service
CVE-2024-26170	No	No	Composite Image File System (CimFS)
CVE-2024-26173	No	No	Kernel
CVE-2024-26174	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2024-26176	No	No	Kernel
CVE-2024-26177	No	No	Kernel
CVE-2024-26178	No	No	Kernel
CVE-2024-26181	No	No	Kernel
CVE-2024-26182	No	No	Kernel
CVE-2024-26185	No	No	Compressed Folder
CVE-2024-26167	No	No	Edge for Android
CVE-2024-21411	No	No	Skype for Consumer
CVE-2024-21426	No	No	SharePoint Server
CVE-2024-26199	No	No	Office
CVE-2024-26204	No	No	Outlook for Android

CVE	Public	Exploited	Product
CVE-2024-21392	No	No	.NET and Visual Studio
CVE-2024-21418	No	No	(SONiC)
CVE-2024-21421	No	No	Azure SDK
CVE-2024-21441	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-21444	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-21450	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-21451	No	No	ODBC Driver
CVE-2024-26190	No	No	QUIC
CVE-2024-26198	No	No	Exchange Server
CVE-2024-26201	No	No	Intune for Android
CVE-2024-26203	No	No	Azure Data Studio
CVE-2024-26161	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-26164	No	No	Django Backend for SQL Server
CVE-2024-21330	No	No	OMI

CVE	Public	Exploited	Product
CVE-2024-21334	No	No	OMI
CVE-2024-21390	No	No	Authenticator
CVE-2024-21400	No	No	Azure Kubernetes Service Confidential Container
CVE-2024-21419	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2024-21448	No	No	Teams for Android
CVE-2024-26166	No	No	WDAC OLE DB provider for SQL Server
CVE-2023-28746	No	No	Intel: CVE-2023-28746 Register File Data Sampling (RFDS)
CVE-2024-26165	No	No	Visual Studio Code