Microsoft

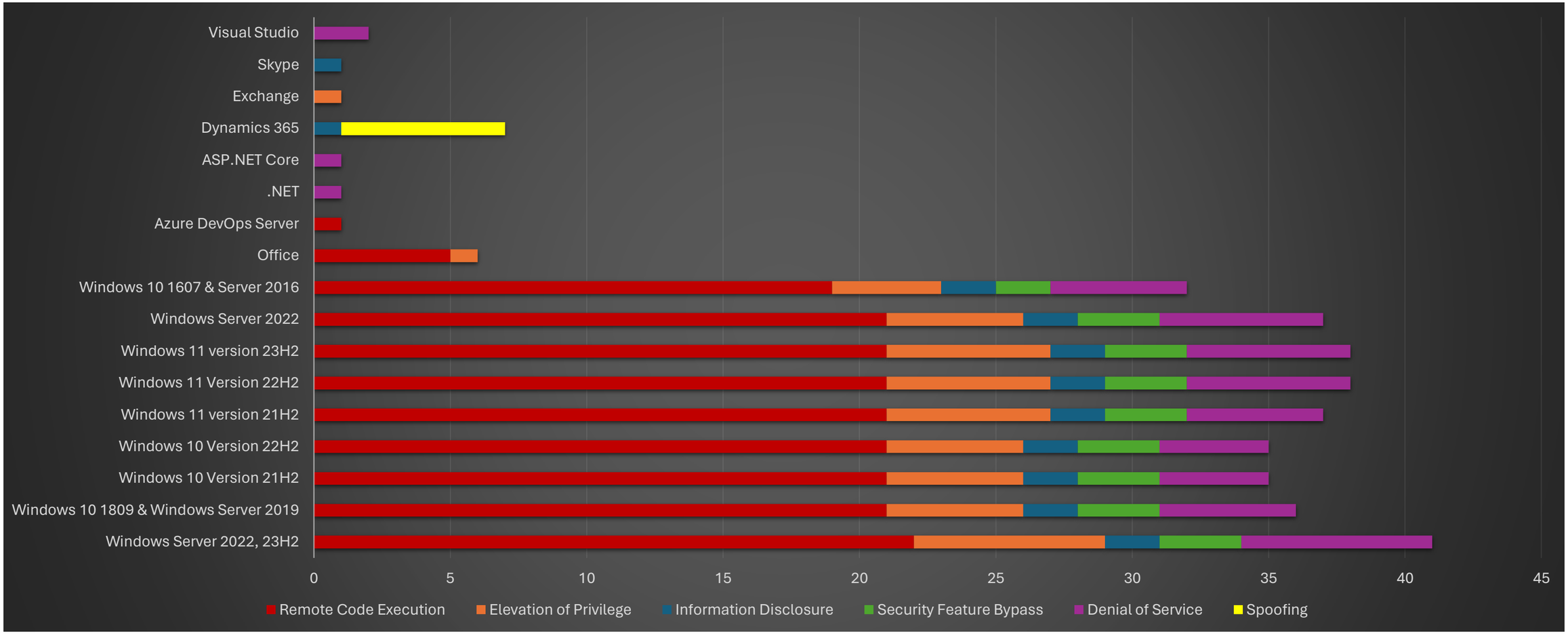
Microsoft Security Release

February 13, 2024

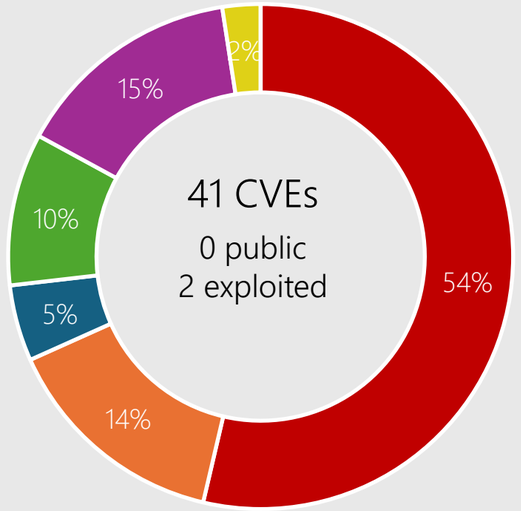
Agenda

- Security Updates
- Product Support Lifecyle
- Other Resources Related to the Release

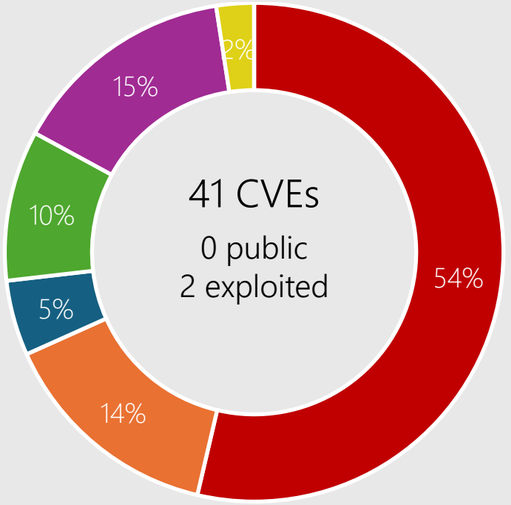
Microsoft Security Release Overview – February 2024



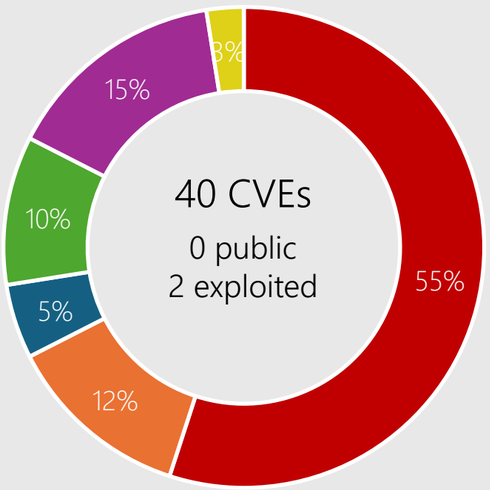
Windows 11, Server 2022



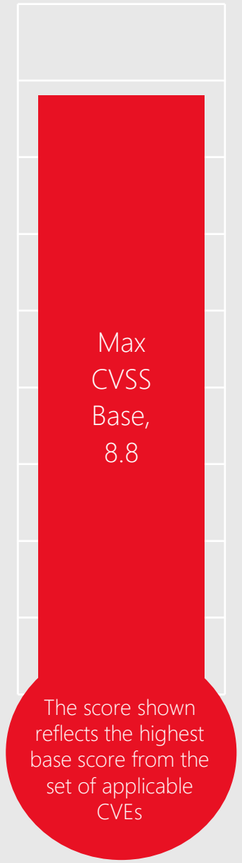
Windows 11 23H2



Windows 11 22H2



Windows Server 2022



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

Affected Components:

See appendix

CVE-2024-21412 Internet Shortcut Files

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 8.1 | 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

CVE-2024-21351 Windows SmartScreen

Impact, Severity, Disclosure

Security Feature Bypass | Moderate | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 7.6| 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-2024-21345 Kernel

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

Server 2022, 23H2 Edition

CVE-2024-21353 WDAC 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.

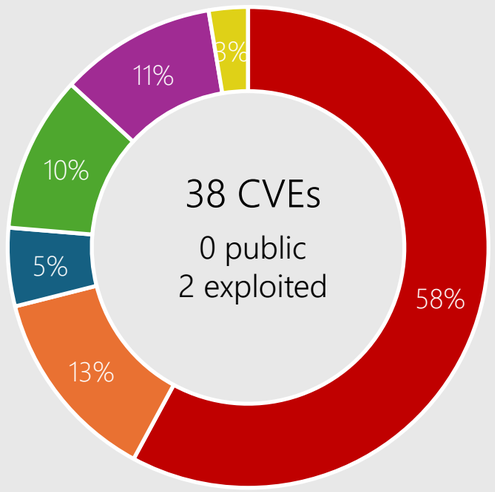
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

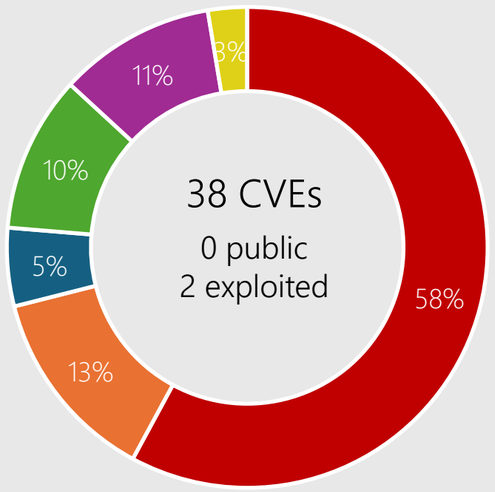
Affected Software

Server 2022, 23H2 Edition

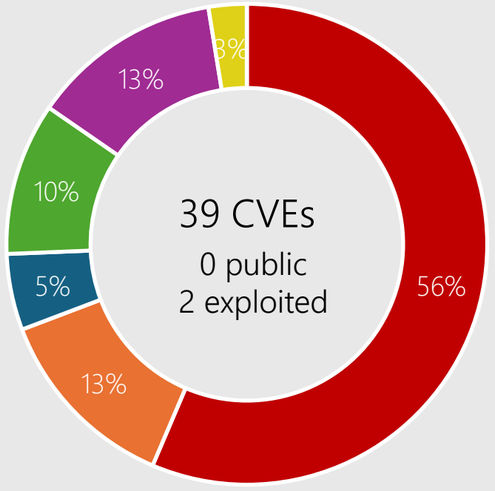
Windows 10



Windows 10 22H2

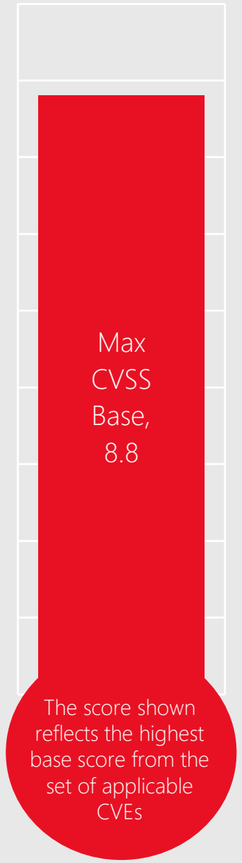


Windows 10 21H2



Windows 10 1809 & Windows Server 2019

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



Affected Components:

See appendix

CVE-2024-21372 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
Server 2022
Server 2019
Server 2016

CVE-2024-21350 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-2024-21349 ActiveX Data Objects

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-2024-21357 Pragmatic General Multicast (PGM)

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Adjacent | Attack Complexity: High | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

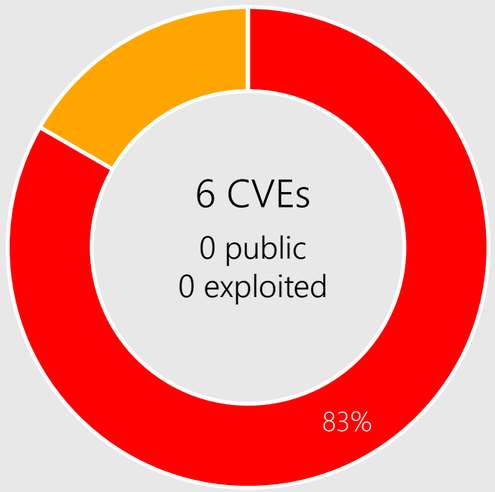
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
Office 2016
Word 2016
Excel 2016
Outlook 2016
PowerPoint 2016
Publisher 2016
Visio 2016
365 Apps Enterprise
Office LTSC 2021
Skype for Business 2016

CVE-2024-21413 Outlook

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

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Office LTSC 2021
Office 2016
Office 2019
365 Apps Enterprise

CVE-2024-20673 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

- Word 2016
- Visio 2016
- Skype Business 2016
- Publisher 2016
- PowerPoint 2016
- Office LTSC 2021
- Office 2019
- Office 2016
- Excel 2016

Other Products

Exchange Server

CVE-2024-21410 | Critical | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 9.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 14, Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23.

Other Products

Dynamics 365

CVE-2024-21380 | Critical | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 Business Central 2023 Release Wave 2, Dynamics 365 Business Central 2023 Release Wave 1, Dynamics 365 Business Central 2022 Release Wave 2.

CVE-2024-21395 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1.

Other Products

Dynamics 365

CVE-2024-21327 | 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 Customer Engagement V9.1.

CVE-2024-21328/21389/21393/21394/21396 | 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

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-21404 | .NET 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: .NET 6.0, .NET 7.0, .NET 8.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.8

CVE-2024-21386 | .NET 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: ASP.NET Core 6.0, ASP.NET Core 7.0, ASP.NET Core 8.0, Visual Studio 2022 version 17.8, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4

Other Products

Azure DevOps Server

CVE-2024-20667 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Azure DevOps Server 2022.1, Azure DevOps Server 2019.1.2, Azure DevOps Server 2020.1.2.

Other Products

Microsoft Defender for Endpoint

CVE-2024-21315 | 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: Defender Endpoint Windows on Windows 10, Defender Endpoint Windows on Windows 10 21H2, Defender Endpoint Windows on Windows 10 22H2, Defender Endpoint Windows on Windows 10 1607, Defender Endpoint Windows on Windows 10 1809, Defender Endpoint Windows on Server 2019, Defender Endpoint Windows on Server 2022, Defender Endpoint Windows on Windows 11 version 21H2, Defender Endpoint Windows on Server 2016, Defender Endpoint Windows on Server 2022, 23H2 Edition, Defender Endpoint Windows on Windows 11 23H2, Defender Endpoint Windows on Windows 11 22H2.

Other Products

Azure Kubernetes Service Confidential Containers

CVE-2024-21376 | Important | Remote Code Execution | 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.

CVE-2024-21403 | 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

Azure Site Recovery

CVE-2024-21364 | Moderate | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 9.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure Site Recovery.

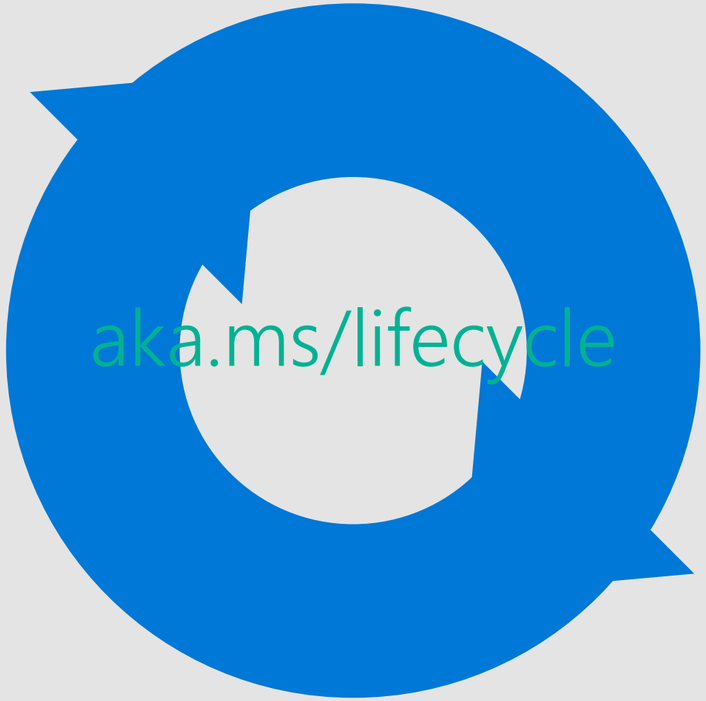
Other Products

Azure

CVE-2024-21329 Azure Connected Machine Agent
CVE-2024-21397 Azure File Sync
CVE-2024-20679 Azure Stack Hub
CVE-2024-21381 Azure Active Directory B2C
CVE-2024-21401 Microsoft Entra Jira Single-Sign-On Plugin

Product Lifecycle Update

End of servicing for Configuration Manager version 2207



Updating the Microsoft Secure Boot Keys

Summary

Microsoft is rolling out an optional Secure Boot DB update to add a new Microsoft Windows UEFI CA 2023 to replace the existing Windows Production 2011 CA.
This DB update will be optional for the February 2024 servicing and preview updates and can be manually applied to devices. Microsoft will slowly rollout this DB update, as we validate devices and firmware compatibility globally. The full DB update's controlled-rollout process to all Windows customers will begin during the 2024 April servicing and preview updates, ahead of the certificate expiration in 2026.

Suggested Actions:

Review the Windows IT Pro blog post to familiarize yourself with the secure boot process, validate the target system is compatible, then proceed with the DB update on select non-critical hardware that is representative of devices in your environment.

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/updating-microsoft-secure-boot-keys/ba-p/4055324

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2024-21338	No	No	Kernel
CVE-2024-21340	No	No	Kernel
CVE-2024-21351	No	Yes	SmartScreen
CVE-2024-21354	No	No	Message Queuing (MSMQ)
CVE-2024-21357	No	No	Pragmatic General Multicast (PGM)
CVE-2024-21371	No	No	Kernel
CVE-2024-21372	No	No	OLE
CVE-2024-20684	No	No	Hyper-V
CVE-2024-21339	No	No	USB Generic Parent Driver
CVE-2024-21341	No	No	Kernel
CVE-2024-21342	No	No	DNS Client
CVE-2024-21343	No	No	Network Address Translation (NAT)
CVE-2024-21344	No	No	Network Address Translation (NAT)

CVE	Public	Exploited	Product
CVE-2024-21345	No	No	Kernel
CVE-2024-21346	No	No	Win32k
CVE-2024-21348	No	No	Internet Connection Sharing (ICS)
CVE-2024-21355	No	No	Message Queuing (MSMQ)
CVE-2024-21356	No	No	Lightweight Directory Access Protocol (LDAP)
CVE-2024-21362	No	No	Kernel
CVE-2024-21363	No	No	Message Queuing (MSMQ)
CVE-2024-21377	No	No	DNS
CVE-2024-21405	No	No	Message Queuing (MSMQ)
CVE-2024-21406	No	No	Printing Service
CVE-2024-21399	No	No	Edge (Chromium-based)

CVE	Public	Exploited	Product
CVE-2024-21379	No	No	Word
CVE-2024-21402	No	No	Outlook
CVE-2024-21413	No	No	Outlook
CVE-2024-20673	No	No	Office
CVE-2024-20695	No	No	Skype for Business
CVE-2024-21378	No	No	Outlook
CVE-2024-21384	No	No	Office OneNote
CVE-2024-21626	No	No	
CVE-2024-20667	No	No	Azure DevOps Server
CVE-2023-50387	No	No	MITRE: CVE-2023-50387 DNS RRSIGs and DNSKEYs validation can be abused to remotely consume DNS server resources
CVE-2024-21327	No	No	Dynamics 365 Customer Engagement Cross-Site Scripting
CVE-2024-21329	No	No	Azure Connected Machine Agent

CVE	Public	Exploited	Product
CVE-2024-21349	No	No	ActiveX Data Objects
CVE-2024-21350	No	No	WDAC OLE DB provider
CVE-2024-21352	No	No	WDAC OLE DB provider
CVE-2024-21358	No	No	WDAC OLE DB provider
CVE-2024-21360	No	No	WDAC OLE DB provider
CVE-2024-21361	No	No	WDAC OLE DB provider
CVE-2024-21366	No	No	WDAC OLE DB provider
CVE-2024-21369	No	No	WDAC OLE DB provider
CVE-2024-21375	No	No	WDAC OLE DB provider
CVE-2024-21381	No	No	Azure Active Directory B2C
CVE-2024-21386	No	No	.NET
CVE-2024-21389	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2024-21393	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2024-21394	No	No	Dynamics 365 Field Service

CVE	Public	Exploited	Product
CVE-2024-21396	No	No	Dynamics 365 Sales
CVE-2024-21401	No	No	Entra Jira Single-Sign-On Plugin
CVE-2024-21404	No	No	.NET
CVE-2024-21420	No	No	WDAC OLE DB provider
CVE-2024-20679	No	No	Azure Stack Hub
CVE-2024-21304	No	No	Trusted Compute Base
CVE-2024-21315	No	No	Defender for Endpoint Protection
CVE-2024-21328	No	No	Dynamics 365 Sales
CVE-2024-21347	No	No	ODBC Driver
CVE-2024-21353	No	No	WDAC ODBC Driver
CVE-2024-21359	No	No	WDAC OLE DB provider
CVE-2024-21364	No	No	Azure Site Recovery
CVE-2024-21365	No	No	WDAC OLE DB provider
CVE-2024-21367	No	No	WDAC OLE DB provider

CVE	Public	Exploited	Product
CVE-2024-21368	No	No	WDAC OLE DB
CVE-2024-21370	No	No	WDAC OLE DB
CVE-2024-21374	No	No	Teams for Android
CVE-2024-21376	No	No	Azure Kubernetes Service Confidential Container
CVE-2024-21380	No	No	Dynamics Business Central/NAV
CVE-2024-21391	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-21395	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2024-21397	No	No	Azure File Sync
CVE-2024-21403	No	No	Azure Kubernetes Service Confidential Container
CVE-2024-21410	No	No	Exchange Server
CVE-2024-21412	No	Yes	Internet Shortcut Files