Microsoft

Microsoft Security Release

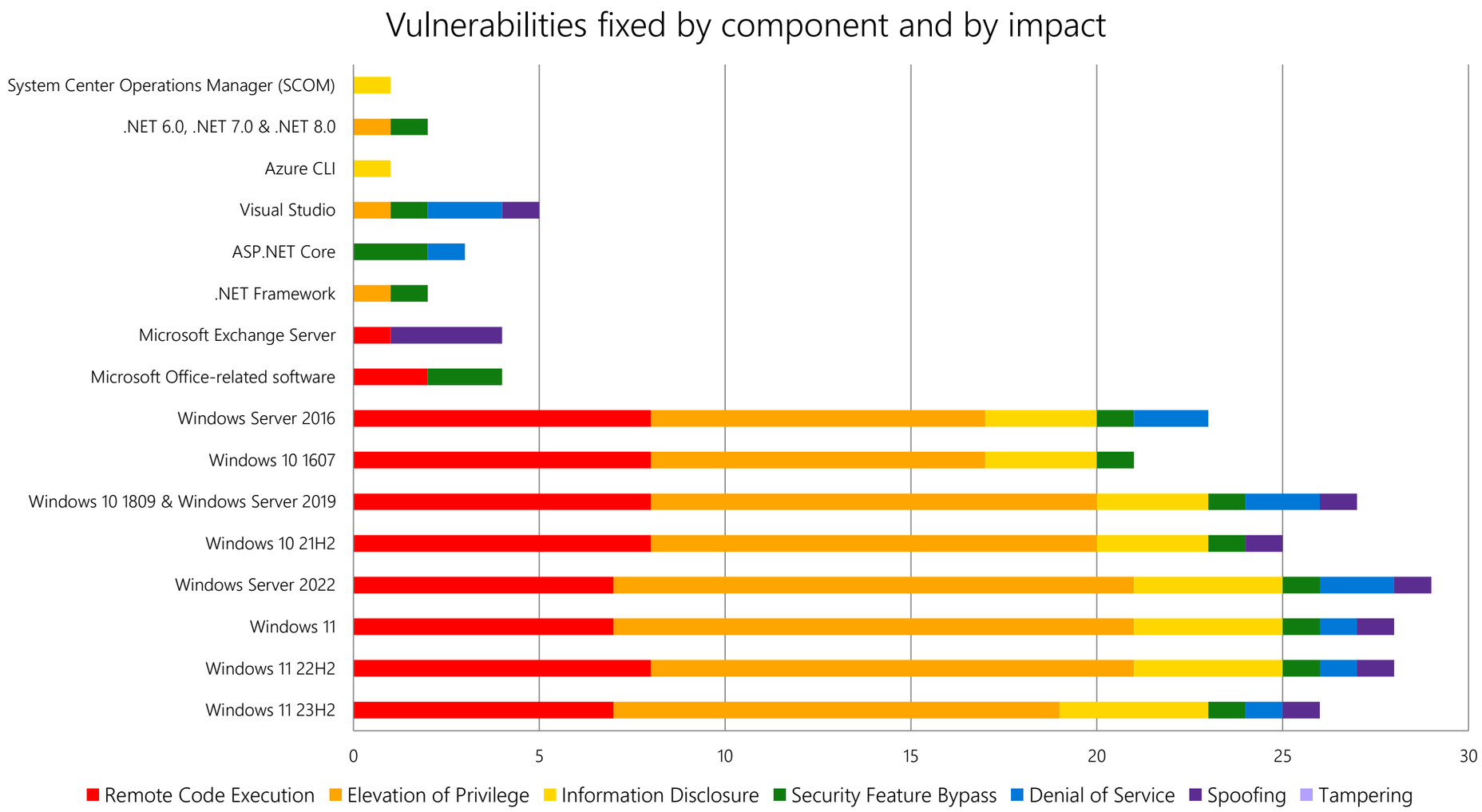
November 14, 2023

Agenda

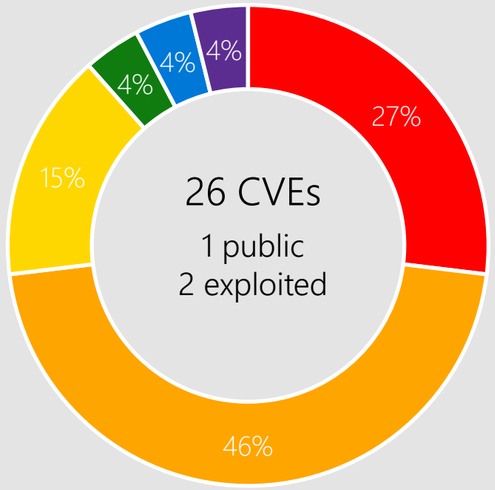
Security Updates

Product Support Lifecyle

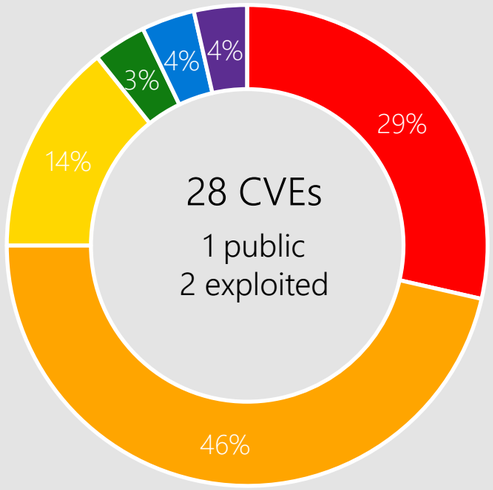
Monthly Security Release Overview - November 2023



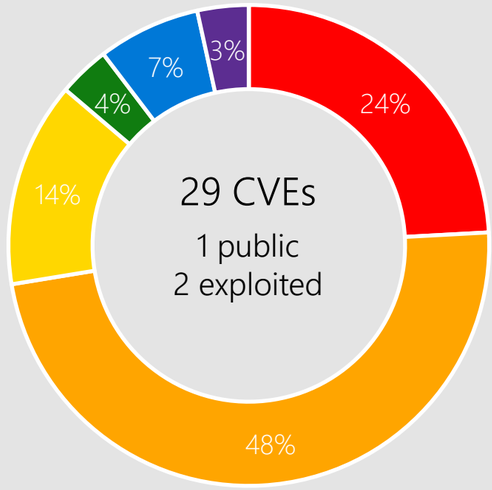
Windows 11, Server 2022



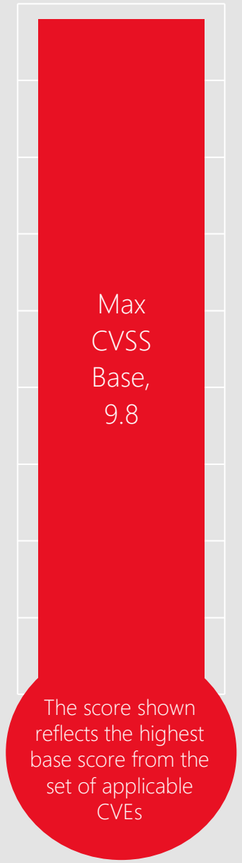
Windows 11 23H2



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-2023-36397 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

The Windows message queuing service, which is a Windows component, needs to be enabled for a system to be exploitable by this vulnerability. This feature can be added via the Control Panel.

You can check to see if there is a service running named Message Queuing and TCP port 1801 is listening on the machine.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 23H2
Windows 11 version 21H2
Server 2022
Server 2022, 23H2 Edition
Server 2019
Windows 10
Server 2016

CVE-2023-36028 PEAP

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

Microsoft Protected Extensible Authentication Protocol (PEAP) is only negotiated with the client if NPS is running on the Windows Server and has a network policy configured that allows PEAP. See CVE entry for details on disallowing the use of PEAP.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 23H2
Windows 11 version 21H2
Server 2022
Server 2022, 23H2 Edition
Server 2019
Windows 10
Server 2016

CVE-2023-36025 SmartScreen

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

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 22H2
- Windows 11 23H2
- Windows 11 version 21H2
- Server 2022
- Server 2022, 23H2 Edition
- Server 2019
- Windows 10
- Server 2016

CVE-2023-36033 DWM Core Library

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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.

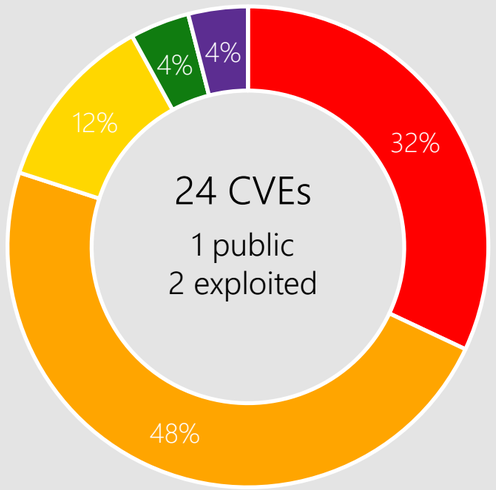
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

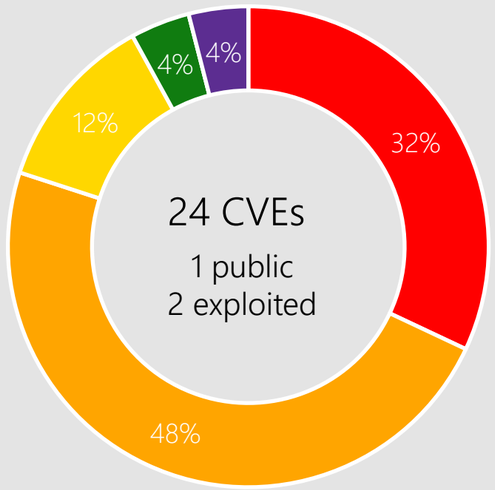
Affected Software

Windows 11 22H2
Windows 11 version 21H2
Windows 11 23H2
Server 2022, 23H2 Edition
Server 2022
Server 2019
Windows 10

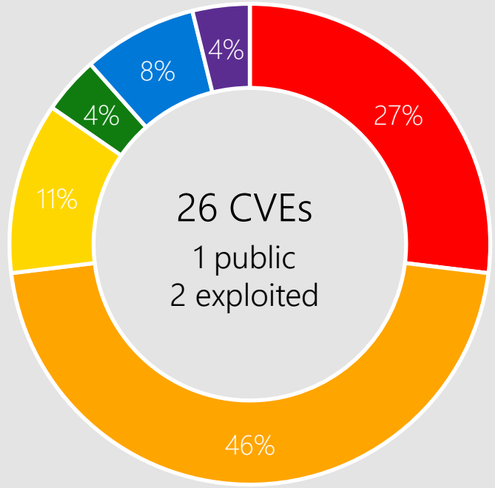
Windows 10



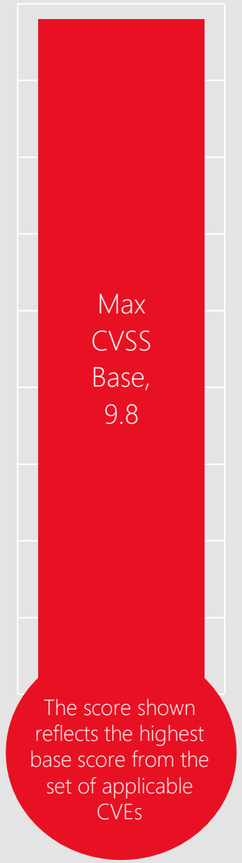
Windows 10 22H2



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:

See Appendix for details

CVE-2023-36400 HMAC Key Derivation

Impact, Severity, Disclosure

Elevation of Privilege | Critical | 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 22H2
- Windows 11 23H2
- Windows 11 version 21H2
- Server 2022
- Server 2022, 23H2 Edition
- Server 2019
- Windows 10
- Server 2016

CVE-2023-36402 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 22H2
- Windows 11 version 21H2
- Windows 11 23H2
- Server 2022
- Server 2022, 23H2 Edition
- Server 2019
- Windows 10
- Server 2016

CVE-2023-36719 Speech API

Impact, Severity, Disclosure

Elevation of Privilege| Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.4 | Attack Vector: Local | 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 22H2
- Windows 11 23H2
- Windows 11 version 21H2
- Server 2022
- Server 2022, 23H2 Edition
- Server 2019
- Windows 10
- Server 2016

CVE-2023-36425 Distributed File System (DFS)

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8 | Attack Vector: Network | Attack Complexity: High | Privileges Required: High | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

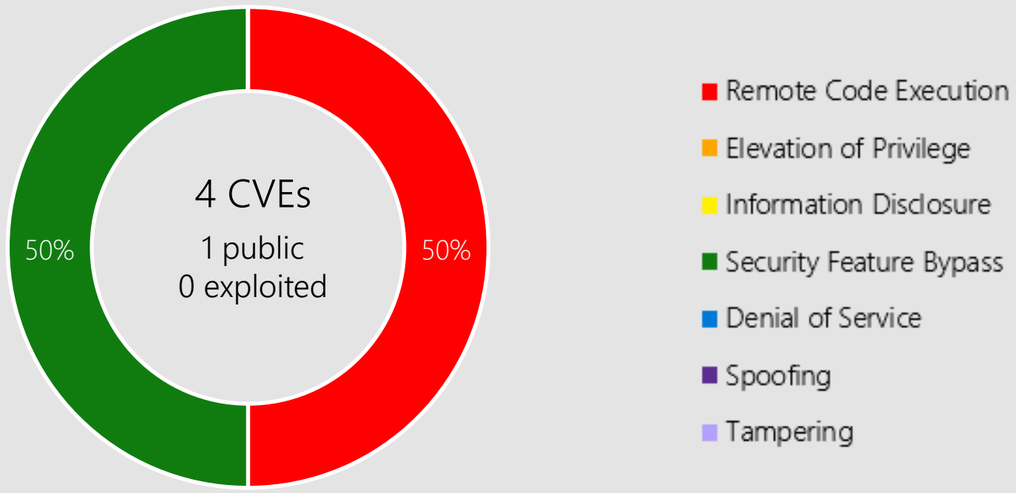
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 23H2
- Windows 11 version 21H2
- Server 2022
- Server 2022, 23H2 Edition
- Server 2019
- Windows 10
- Server 2016

Microsoft Office



Microsoft Office-related software

Products:

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

CVE-2023-36041 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
Excel 2016
Office LTSC for Mac 2021
Office 2019
365 Apps Enterprise

CVE-2023-36045 Office Graphics

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 for Mac 2021
Office LTSC 2021
Office 2019
365 Apps Enterprise

CVE-2023-38177 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 6.1 | Attack Vector: Adjacent | 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

SharePoint Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

Other Products

Exchange Server

CVE-2023-36439 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23.

CVE-2023-36050 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

Other Products

Exchange Server

CVE-2023-36035 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 13, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

CVE-2023-36039 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 13, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

Other Products

System Center Operations Manager

CVE-2023-36043 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: System Center Operations Manager (SCOM) 2022, System Center Operations Manager (SCOM) 2019, System Center Operations Manager (SCOM) 2016.

Other Products

Dynamics 365

CVE-2023-36031 | 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.

CVE-2023-36410 | 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

Dynamics 365

CVE-2023-36016 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-36030 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Dynamics 365 Sales

CVE-2023-36007 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score: 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Send Customer Voice survey from Dynamics 365 app

Developer Tools

Microsoft .NET Framework, ASP.NET Core, .NET, Visual Studio

CVE-2023-36560 | ASP.NET Security Feature Bypass Vulnerability

Base CVSS: 8.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: Microsoft .NET Framework (2.0, 3.0, 3.5, 3.5.1, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1)

CVE-2023-36049 | .NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability

Base CVSS: 7.6 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: Microsoft.NET Framework (2.0, 3.0, 3.5, 3.5.1, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1), NET 6.0, 7.0, & 8.0, Visual Studio 2022

CVE-2023-36558 | ASP.NET Core - Security Feature Bypass Vulnerability

Base CVSS: 6.2 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: ASP.NET Core 6.0, 7.0, & 8.0, .NET 6.0, 7.0 & 8.0, Visual Studio 2022

Developer Tools

ASP.NET Core 8.0, Visual Studio Code, Visual Studio

CVE-2023-36038 | ASP.NET Core Denial of Service Vulnerability

Base CVSS: 8.2 | **Max Severity**: Important | **Public**: Yes | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: ASP.NET Core 8.0, Visual Studio 2022

CVE-2023-36018 | . Visual Studio Code Jupyter Extension Spoofing Vulnerability

Base CVSS: 7.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: Jupyter Extension for Visual Studio Code

CVE-2023-36042 | Visual Studio Denial of Service Vulnerability

Base CVSS: 6.2 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Visual Studio 2022, Visual Studio 2019

Other Products

Windows Defender Antimalware Platform

CVE-2023-36422 | 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 Defender Antimalware Platm.

Other Products

Azure CLI

CVE-2023-36052 | Critical | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 8.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure CLI commands related to App Service family (Web Apps, Functions, etc.)
More Information: Microsoft guidance regarding credentials leaked to Github Actions logs through Azure CLI

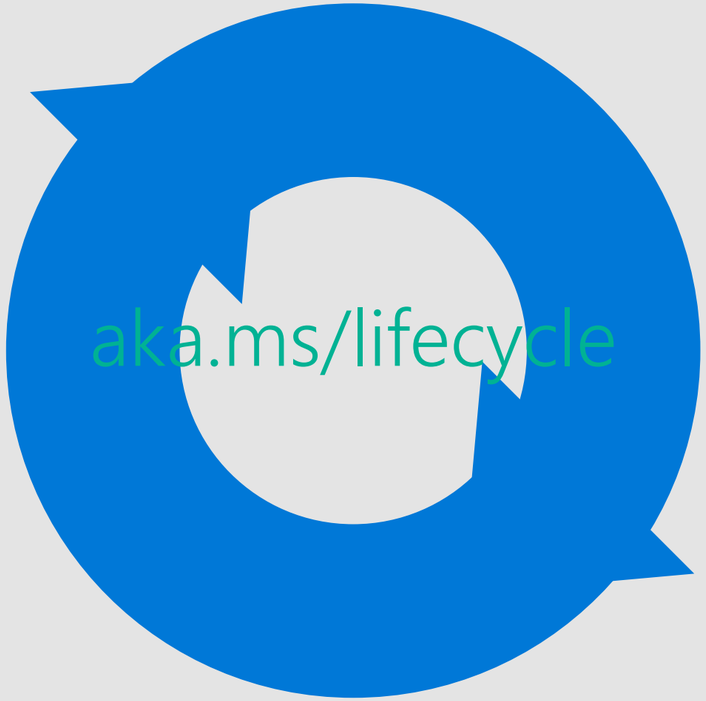
Other Products

Azure

CVE-2023-36437 Azure Pipelines Agent
CVE-2023-38151 Host Integration Server 2020 and OLE DB Provider for DB2 V7
CVE-2023-36021 On-Prem Data Gateway

Product Lifecycle Update

No Products Reaching End Of Support in November



Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-36719	No	No	SAPI
CVE-2023-36705	No	No	Installer
CVE-2023-36428	No	No	Local Security Authority Subsystem Service
CVE-2023-36427	No	No	Hyper-V
CVE-2023-36425	No	No	DFS
CVE-2023-36424	No	No	CLFS
CVE-2023-36422	No	No	Defender
CVE-2023-36036	Yes	No	Cloud Files Mini Filter Driver
CVE-2023-36017	No	No	Scripting Engine
CVE-2023-36408	No	No	Hyper-V
CVE-2023-36407	No	No	Hyper-V
CVE-2023-36406	No	No	Hyper-V
CVE-2023-36405	No	No	Kernel
CVE-2023-36404	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-36403	No	No	Kernel
CVE-2023-36400	No	No	HMAC Key Derivation
CVE-2023-36399	No	No	Storage
CVE-2023-36398	No	No	NTFS
CVE-2023-36397	No	No	PGM
CVE-2023-36396	No	No	Compressed Folder
CVE-2023-36395	No	No	Deployment Services
CVE-2023-36394	No	No	Search Service
CVE-2023-36393	No	No	User Interface Application Core
CVE-2023-36392	No	No	DHCP Server Service
CVE-2023-36046	No	No	Authentication
CVE-2023-36047	No	No	Authentication
CVE-2023-36045	No	No	Office Graphics
CVE-2023-36028	No	No	PEAP

CVE	Public	Exploited	Product
CVE-2023-36437	No	No	Azure DevOps Server
CVE-2023-36423	No	No	Remote Registry Service
CVE-2023-36410	No	No	Dynamics 365 (on-prem)
CVE-2023-36052	No	No	Azure CLI REST Command
CVE-2023-36043	No	No	OMI
CVE-2023-36558	No	No	ASP.NET Core -
CVE-2023-36439	No	No	Exchange Server
CVE-2023-36402	No	No	WDAC OLE DB provider for SQL Server
CVE-2023-36401	No	No	Remote Registry Service
CVE-2023-36049	No	No	.NET, .NET Framework, and Visual Studio
CVE-2023-24023	No	No	Bluetooth
CVE-2023-36050	No	No	Exchange Server
CVE-2023-36039	No	No	Exchange Server
CVE-2023-36042	No	No	Visual Studio

CVE	Public	Exploited	Product
CVE-2023-36038	Yes	No	ASP.NET Core
CVE-2023-36035	No	No	Exchange Server
CVE-2023-36030	No	No	Dynamics 365 Sales
CVE-2023-36031	No	No	Dynamics 365 (on-prem)
CVE-2023-36021	No	No	On-Prem Data Gateway
CVE-2023-36016	No	No	Dynamics 365 (on-prem)
CVE-2023-36018	No	No	Visual Studio Code Jupyter Extension

CVE	Public	Exploited	Product
CVE-2023-36033	Yes	Yes	DWM Core Library
CVE-2023-36025	No	Yes	SmartScreen
CVE-2023-36034	No	No	Edge (Chromium-based)
CVE-2023-36024	No	No	Edge (Chromium-based)
CVE-2023-36029	No	No	Edge (Chromium-based)
CVE-2023-36022	No	No	Edge (Chromium-based)
CVE-2023-36027	No	No	Edge (Chromium-based)
CVE-2023-36014	No	No	Edge (Chromium-based)

CVE	Public	Exploited	Product
CVE-2023-36413	Yes	No	Office
CVE-2023-38177	No	No	SharePoint Server
CVE-2023-36041	No	No	Excel
CVE-2023-36037	No	No	Excel
CVE-2023-38151	No	No	Host Integration Server 2020
CVE-2023-36560	No	No	ASP.NET