Microsoft

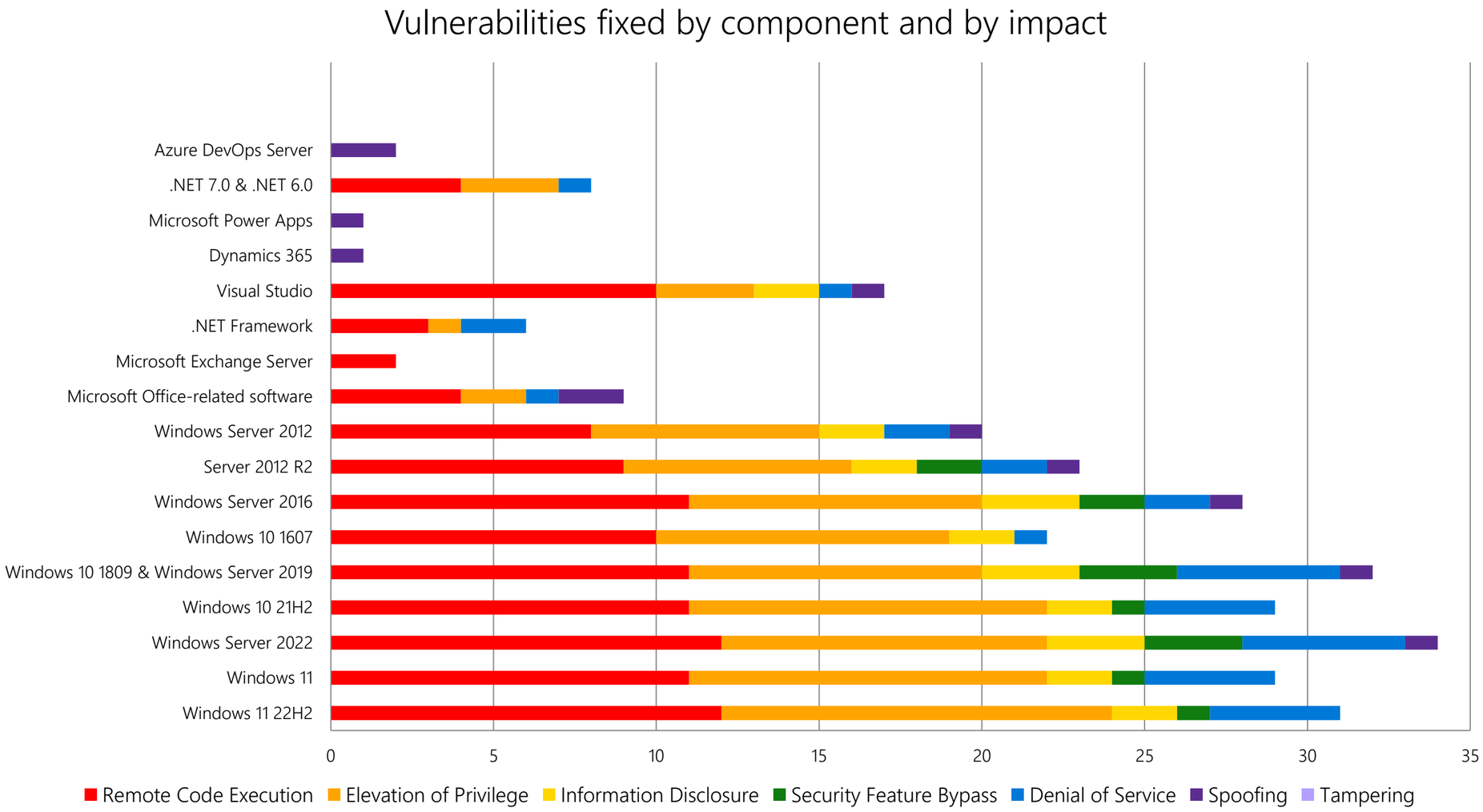
Microsoft Security Release

June 13, 2023

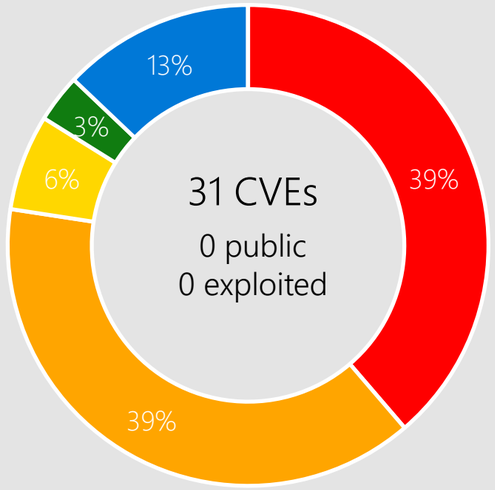
Agenda

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

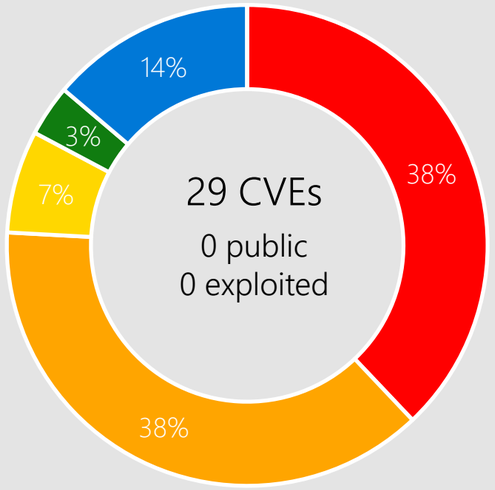
Monthly Security Release Overview - June 2023



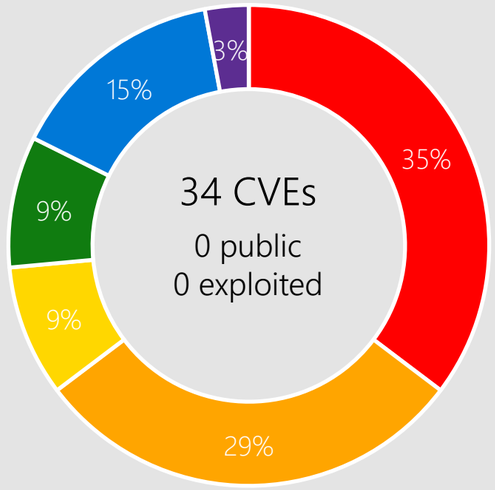
Windows 11, Server 2022



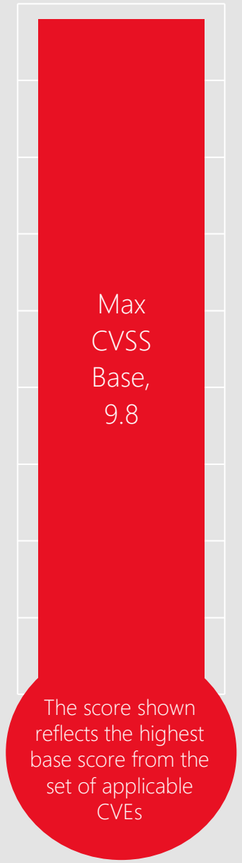
Windows 11 22H2



Windows 11



Windows Server 2022



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

Affected Components:

Please see appendix for details

CVE-2023-29363 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 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-29373 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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-32009 Windows CTF

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.

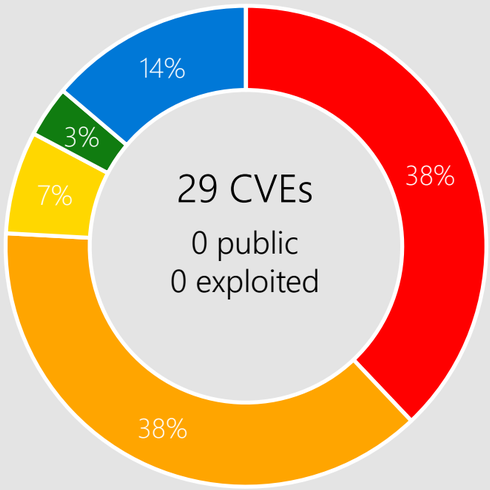
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

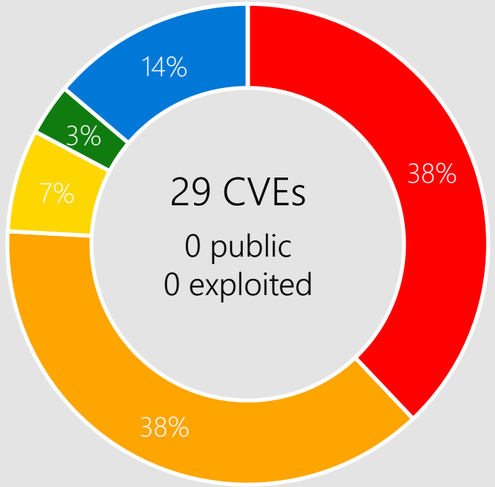
Affected Software

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

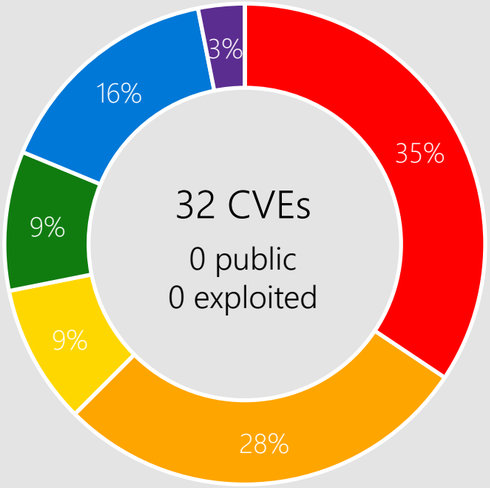
Windows 10



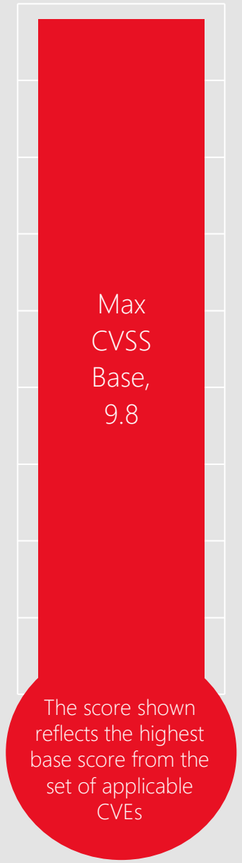
Windows 10 22H2



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:

Please see appendix for details

CVE-2023-29372 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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-29351 Group Policy

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.1 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

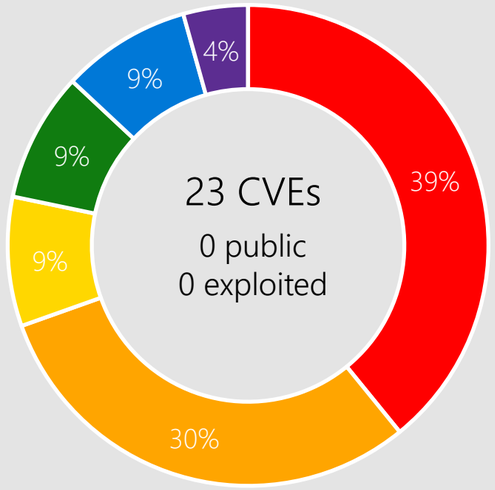
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

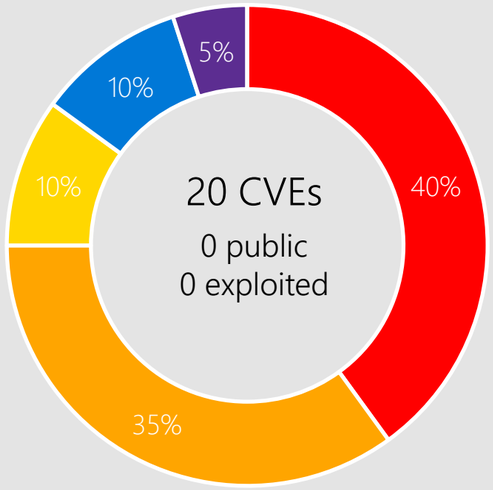
Affected Software

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

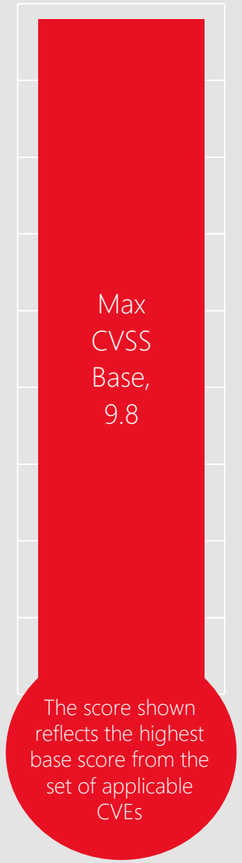
Server 2012 R2, and Server 2012



Server 2012 R2



Windows Server 2012



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

Affected Components:

Authentication
DHCP Server Service
DNS
Filtering Platform
GDI
Group Policy
Installer
iSCSI Discovery Service
iSCSI Target WMI Provider
Media
NTFS
ODBC Driver
PostScript Printer Driver
Pragmatic General Multicast (PGM)
Remote Desktop Client
Remote Procedure Call Runtime
Server Service
SMB Witness Service

CVE-2023-29362 RD Client

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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-29358 GDI

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.

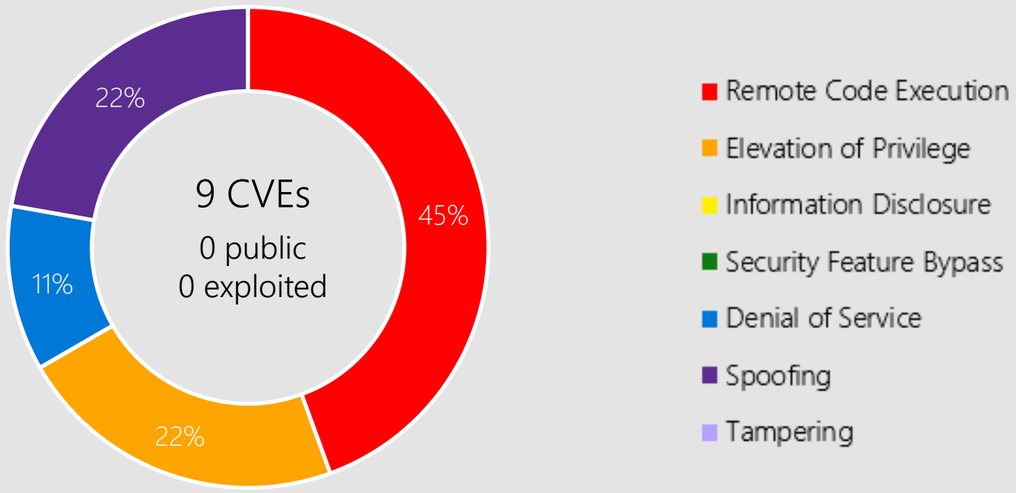
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- 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
Outlook 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
OneNote Universal
SharePoint Server Subscription Edition

CVE-2023-29357 SharePoint Server

Impact, Severity, Disclosure

Elevation of Privilege | 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

Customers who have enabled the AMSI integration feature and use Microsoft Defender across their SharePoint Server farm(s) are protected from this vulnerability. For more information, see Configure AMSI integration with SharePoint Server.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

SharePoint Server 2019

CVE-2023-33131 Outlook

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

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

CVE-2023-33146 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

Office LTSC for Mac 2021
365 Apps Enterprise
Office 2019 for Mac

CVE-2023-32029 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

Exchange Server

CVE-2023-28310 | 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 13, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

CVE-2023-32031 | 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: Exchange Server 2019 Cumulative Update 13, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

Other Products

Dynamics 365

CVE-2023-24896 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 for Finance & Operations

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-24897 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET 7.0, .NET 6.0., also affects .NET Framework and Visual Studio

CVE-2023-24895 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET 7.0, .NET 6.0., also affects .NET Framework and Visual Studio

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-33126 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET 7.0, .NET 6.0., also affects Visual Studio

CVE-2023-33128 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET 7.0, .NET 6.0., also affects Visual Studio

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-24936 | Moderate | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET 7.0, .NET 6.0., also affects .NET Framework and Visual Studio

CVE-2023-29331 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET 7.0, .NET 6.0., also affects .NET Framework and Visual Studio

Other Products

.NET 7.0

CVE-2023-32032 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: .NET 7.0., also affects Visual Studio

Other Products

.NET Framework

CVE-2023-24897 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 4.8 on Server 2012 R2, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 4.8 on Windows 10 1607, also affects .NET 6.0, .NET 7.0 and Visual Studio

Other Products

.NET Framework

CVE-2023-24895 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 4.8 on Windows 10 1607, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2012 R2, also affects .NET 7.0, 6.0 and Visual Studio

Other Products

.NET Framework

CVE-2023-29326 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.7.2 on Server 2019.

Other Products

.NET Framework

CVE-2023-29331 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 4.8 on Windows 10 1607, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 4.8 on Server 2012 R2, also affects .NET 6.0, .NET 7.0 and Visual Studio

Other Products

.NET Framework

CVE-2023-32030 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 4.8 on Server 2012 R2, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2.

Other Products

.NET Framework

CVE-2023-24936 | Moderate | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 1607, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Server 2016, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Server 2012, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 4.8 on Server 2016, .NET Framework 4.8 on Server 2012 R2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.8 on Server 2019, also affects .NET 7.0, .NET 6.0., and Visual Studio 2022

Other Products

Visual Studio

CVE-2023-24897 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2013 Update 5, Visual Studio 2015 Update 3. Also affects .NET 7.0, .NET 6.0, and .NET Framework

CVE-2023-24895 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, also affects .NET 7.0, .NET 6.0, and .NET Framework

Other Products

Visual Studio

CVE-2023-33126 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, .NET 7.0, .NET 6.0.

CVE-2023-33128 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.0, .NET 7.0, .NET 6.0.

Other Products

Visual Studio

CVE-2023-33135 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0.

CVE-2023-32032 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.2, .NET 7.0.

Other Products

Visual Studio

CVE-2023-24936 | Moderate | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.5, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, also affects .NET 7.0, .NET 6.0, and .NET Framework

CVE-2023-33139 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2013 Update 5, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2015 Update 3, Visual Studio 2022 version 17.2, 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

Visual Studio

CVE-2023-29331 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, also affects .NET 7.0, .NET 6.0, and .NET Framework

CVE-2023-33144 | Important | Spoofing | 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

Visual Studio

CVE-2023-25652 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25652

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-27909 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27909

Products: Visual Studio 2013 Update 5, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2015 Update 3, Visual Studio 2022 version 17.2, 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

Visual Studio

CVE-2023-27911 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27911

Products: Visual Studio 2015 Update 3, Visual Studio 2013 Update 5, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, 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).

CVE-2023-29007 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29007

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Visual Studio

CVE-2023-29011 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29011

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-29012 | Important | Remote Code Execution | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29012

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Visual Studio

CVE-2023-25815 | Important | Spoofing | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25815

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-27910 | Important | Information Disclosure | Public: No | Exploited: No

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27910

Products: Visual Studio 2013 Update 5, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2015 Update 3, Visual Studio 2022 version 17.2, 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

Microsoft Power Apps

CVE-2023-32024 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 3
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Power Apps.

Other Products

Azure DevOps Server

CVE-2023-21565 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure DevOps Server 2020.1.2, Azure DevOps Server 2022, Azure DevOps Server 2022.0.1.

CVE-2023-21569 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Azure DevOps Server 2020.1.2, Azure DevOps Server 2022, Azure DevOps Server 2022.0.1.

Other Products

Nuget, YARP, Sysinternals

CVE-2023-29337 Nuget 5.0.2

CVE-2023-33141 YARP 2.0

CVE-2023-29353 Windows Sysinternals Process Monitor

Product Lifecycle Update

Windows 10 Semi-Annual Channel
end of service

Windows 10 21H2 Home & Pro

Microsoft

Questions?

Appendix

Microsoft

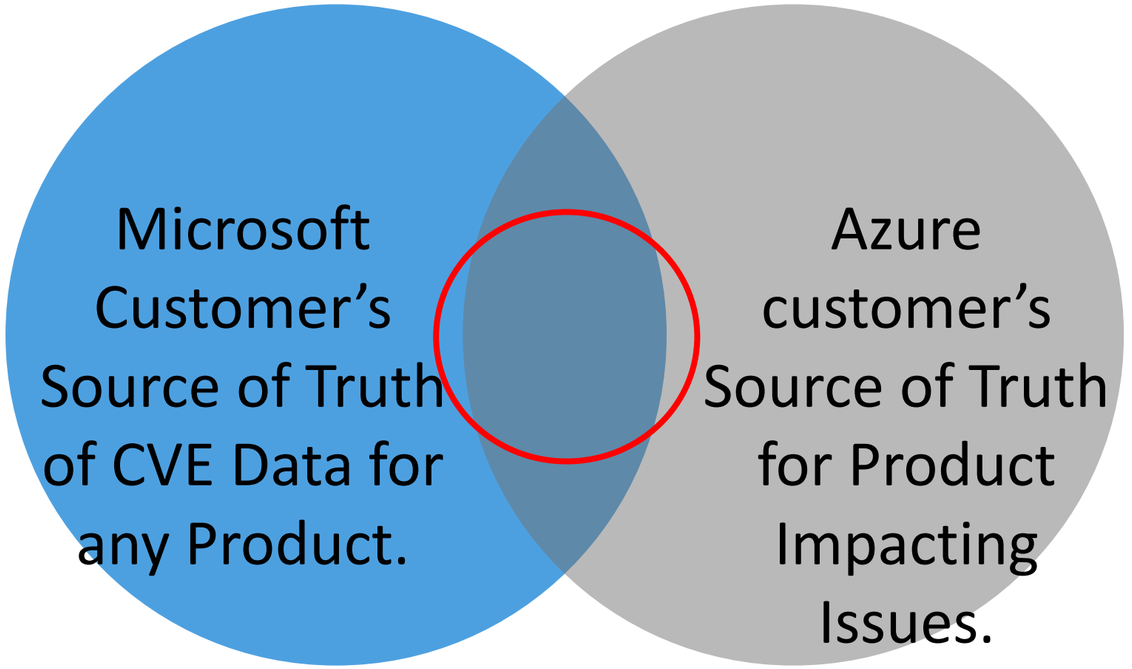
Announcement:

Azure CVE notifications now provided via Azure Service Health Alerts

Team:
MSRC Security Release

Speaker:
Justin Mourfield - Program Manager 2

Current CVE Communication Process

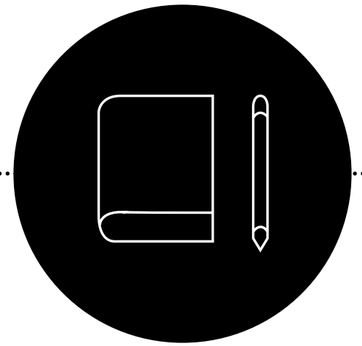


- Opt-in notification method
- Email & RSS Feed
- Customer and product agnostic

- Enabled by default
- Customizable alerting
- Customer and product specific

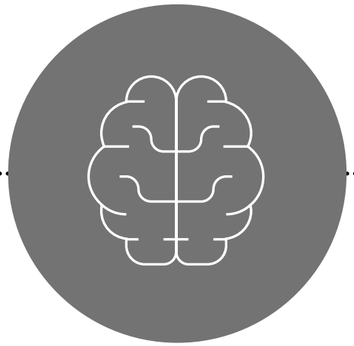
What’s New?

Identify Azure subscriptions



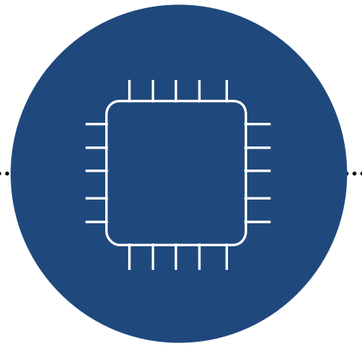
MSRC and Product Engineering identify customers required to take an action to protect their resources against a CVE.

Publicly Disclose CVE



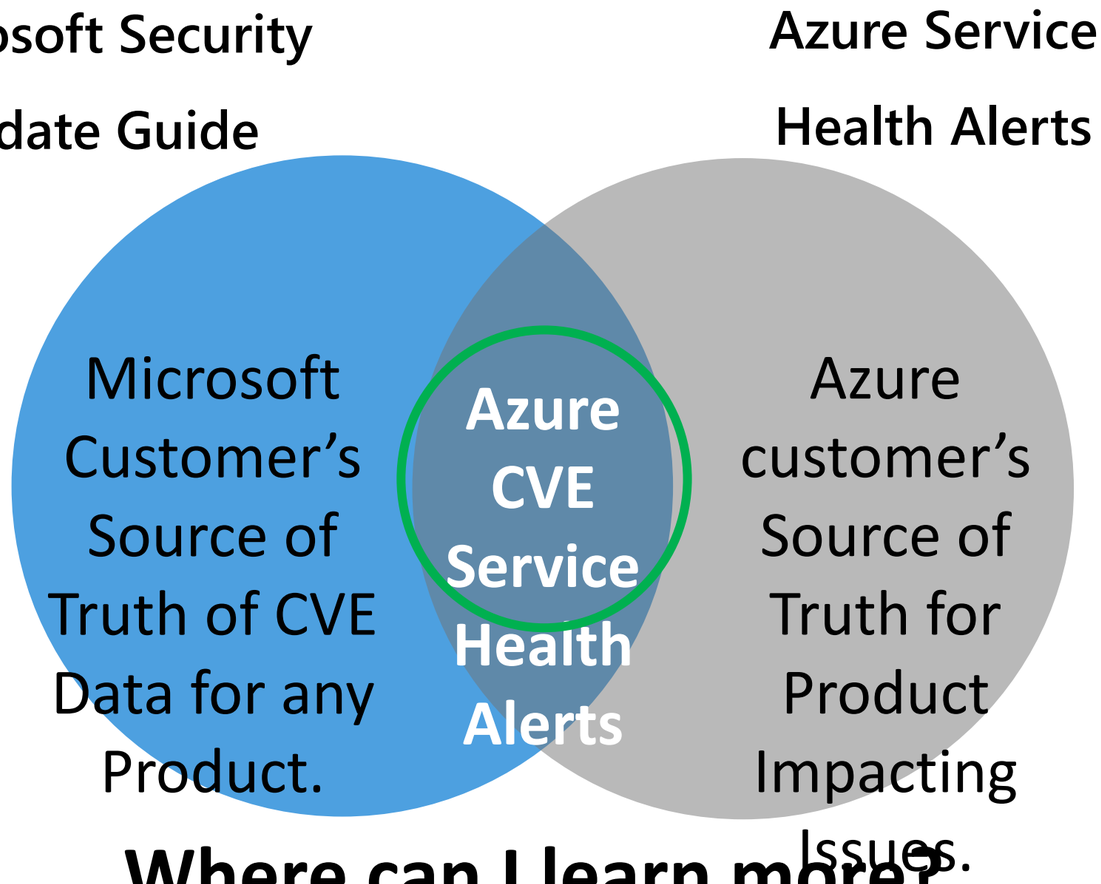
CVEs are published to the Microsoft Security Update Guide on Patch Tuesday or if required for an out-of-band (OOB) disclosure.

Publish Azure Service Health Alert



Customers who must perform an action to reduce the risk posed by a CVE receive a “Security Advisory” via Azure Service Health.

New CVE Communication Process



Where can I learn more?

- Understanding Service Health communications for Azure vulnerabilities
- Azure Service Health Overview
- Stay informed about Azure security issues - Azure Service Health

CVE	Public	Exploited	Product
CVE-2023-24937	No	No	CryptoAPI
CVE-2023-24938	No	No	CryptoAPI
CVE-2023-29353	No	No	Sysinternals Process Monitor for
CVE-2023-29346	No	No	NTFS
CVE-2023-29351	No	No	Group Policy
CVE-2023-29352	No	No	Remote Desktop
CVE-2023-29355	No	No	DHCP Server Service
CVE-2023-29358	No	No	GDI
CVE-2023-29359	No	No	GDI
CVE-2023-29360	No	No	TPM Device Driver
CVE-2023-29361	No	No	Cloud Files Mini Filter Driver
CVE-2023-29363	No	No	Pragmatic General Multicast (PGM)
CVE-2023-29364	No	No	Authentication
CVE-2023-29365	No	No	Media

CVE	Public	Exploited	Product
CVE-2023-29366	No	No	Geolocation Service
CVE-2023-29367	No	No	iSCSI Target WMI Provider
CVE-2023-29368	No	No	Filtering Platform
CVE-2023-29369	No	No	Remote Procedure Call Runtime
CVE-2023-29370	No	No	Media
CVE-2023-29371	No	No	GDI
CVE-2023-29373	No	No	ODBC Driver
CVE-2023-32008	No	No	Resilient File System (ReFS)
CVE-2023-32009	No	No	Collaborative Translation Framework
CVE-2023-32010	No	No	Bus Filter Driver
CVE-2023-32011	No	No	iSCSI Discovery Service
CVE-2023-32012	No	No	Container Manager Service
CVE-2023-32013	No	No	Hyper-V
CVE-2023-32014	No	No	Pragmatic General Multicast (PGM)

CVE	Public	Exploited	Product
CVE-2023-32015	No	No	Pragmatic General Multicast (PGM)
CVE-2023-32016	No	No	Installer
CVE-2023-32018	No	No	Hello
CVE-2023-32019	No	No	Kernel
CVE-2023-32020	No	No	DNS
CVE-2023-32021	No	No	SMB Witness Service
CVE-2023-32022	No	No	Server Service
CVE-2023-3079	No	No	Chromium: CVE-2023-3079 Type Confusion in V8
CVE-2023-29345	No	No	Edge (Chromium-based)
CVE-2023-33143	No	No	Edge (Chromium-based)
CVE-2023-33145	No	No	Edge (Chromium-based)
CVE-2023-2929	No	No	Chromium: CVE-2023-2929 Out of bounds write in Swiftshader
CVE-2023-2930	No	No	Chromium: CVE-2023-2930 Use after free in

CVE	Public	Exploited	Product
CVE-2023-2932	No	No	Chromium: CVE-2023-2932 Use after free in PDF
CVE-2023-2933	No	No	Chromium: CVE-2023-2933 Use after free in PDF
CVE-2023-2934	No	No	Chromium: CVE-2023-2934 Out of bounds memory access in Mojo
CVE-2023-2935	No	No	Chromium: CVE-2023-2935 Type Confusion in V8
CVE-2023-2936	No	No	Chromium: CVE-2023-2936 Type Confusion in V8
CVE-2023-2937	No	No	Chromium: CVE-2023-2937 Inappropriate implementation in Picture In Picture
CVE-2023-2938	No	No	Chromium: CVE-2023-2938 Inappropriate implementation in Picture In Picture

CVE	Public	Exploited	Product
CVE-2023-33129	No	No	SharePoint
CVE-2023-33130	No	No	SharePoint Server
CVE-2023-33131	No	No	Outlook
CVE-2023-33132	No	No	SharePoint Server
CVE-2023-33133	No	No	Excel
CVE-2023-33140	No	No	OneNote
CVE-2023-33142	No	No	SharePoint Server
CVE-2023-28310	No	No	Exchange Server
CVE-2023-24896	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2023-24897	No	No	.NET, .NET Framework, and Visual Studio
CVE-2023-29326	No	No	.NET Framework
CVE-2023-32024	No	No	Power Apps
CVE-2023-32031	No	No	Exchange Server
CVE-2023-33139	No	No	Visual Studio

CVE	Public	Exploited	Product
CVE-2023-21565	No	No	Azure DevOps Server
CVE-2023-21569	No	No	Azure DevOps Server
CVE-2023-24895	No	No	.NET, .NET Framework, and Visual Studio
CVE-2023-24936	No	No	.NET, .NET Framework, and Visual Studio
CVE-2023-29331	No	No	.NET, .NET Framework, and Visual Studio
CVE-2023-29337	No	No	NuGet Client
CVE-2023-29012	No	No	GitHub: CVE-2023-29012 Git CMD erroneously executes `doskey.exe` in current directory, if it exists
CVE-2023-29011	No	No	GitHub: CVE-2023-29011 The config file of `connect.exe` is susceptible to malicious placing
CVE-2023-25815	No	No	GitHub: CVE-2023-25815 Git looks for localized

CVE	Public	Exploited	Product
CVE-2023-32030	No	No	.NET and Visual Studio
CVE-2023-32032	No	No	.NET and Visual Studio
CVE-2023-33126	No	No	.NET and Visual Studio
CVE-2023-33128	No	No	.NET and Visual Studio
CVE-2023-33135	No	No	.NET and Visual Studio
CVE-2023-27909	No	No	AutoDesk: CVE-2023-27909 Out-Of-Bounds Write in Autodesk® FBX® SDK 2020 or prior
CVE-2023-27910	No	No	AutoDesk: CVE-2023-27910 stack buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior
CVE-2023-27911	No	No	AutoDesk: CVE-2023-27911 Heap buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior
CVE-2023-33141	No	No	Yet Another Reverse Proxy