Microsoft

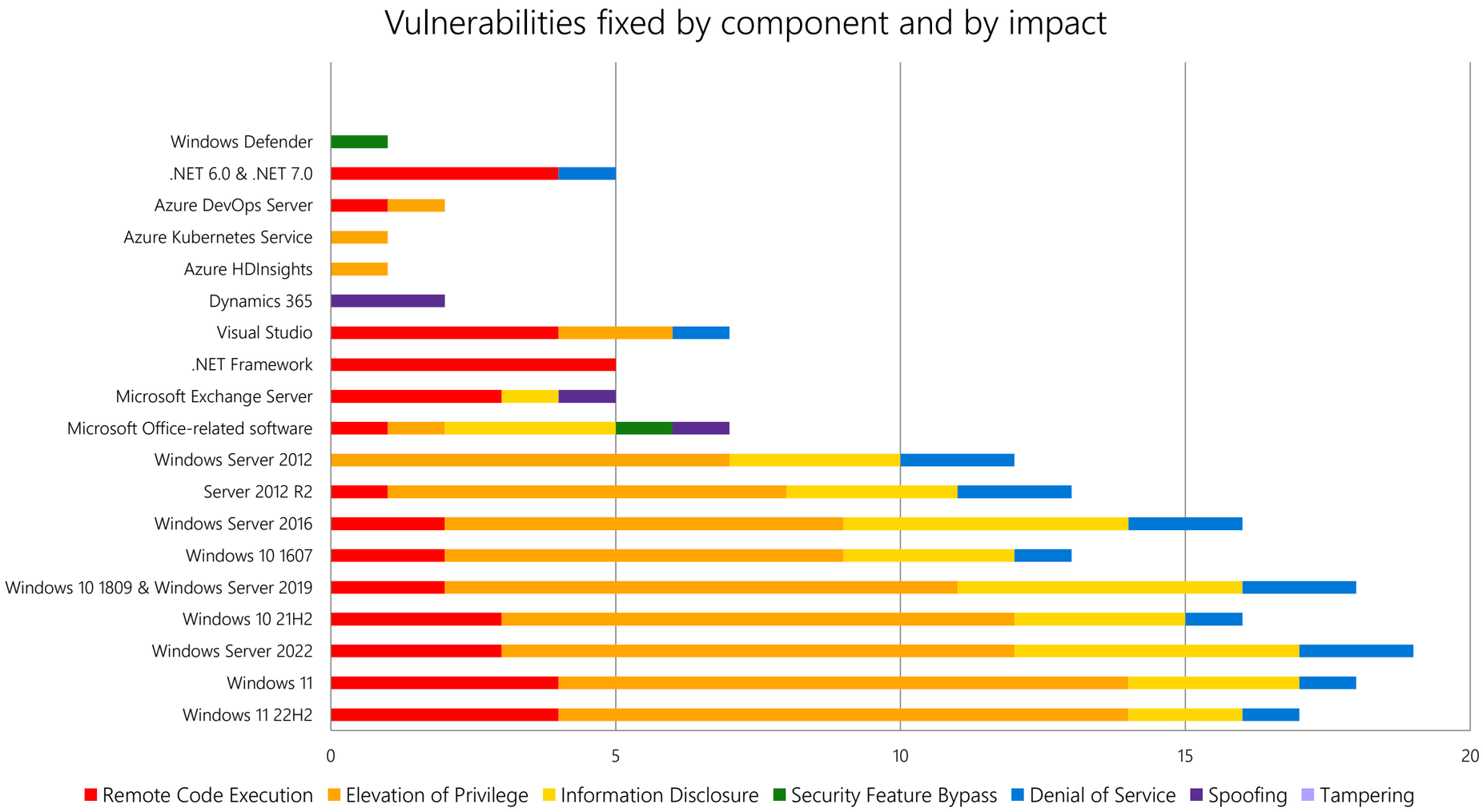
Microsoft Security Release

September 12, 2023

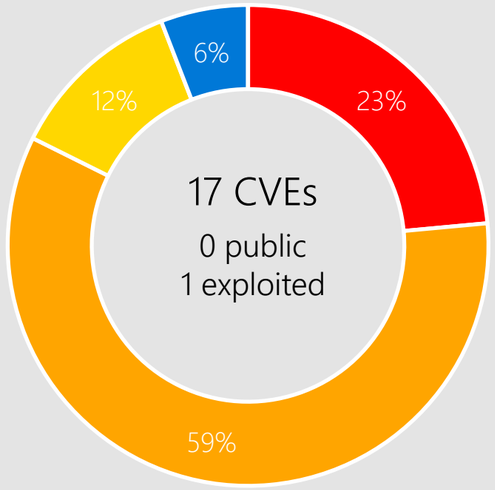
Agenda

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

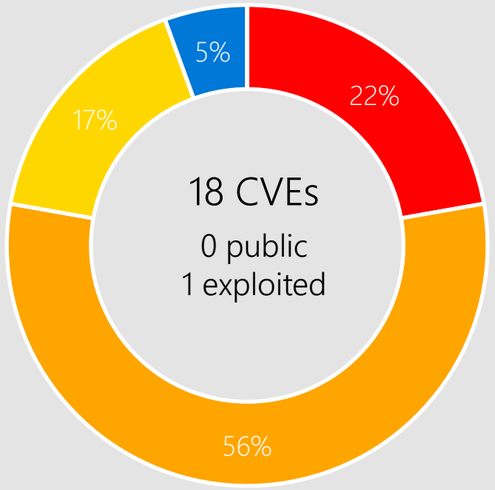
Monthly Security Release Overview - September 2023



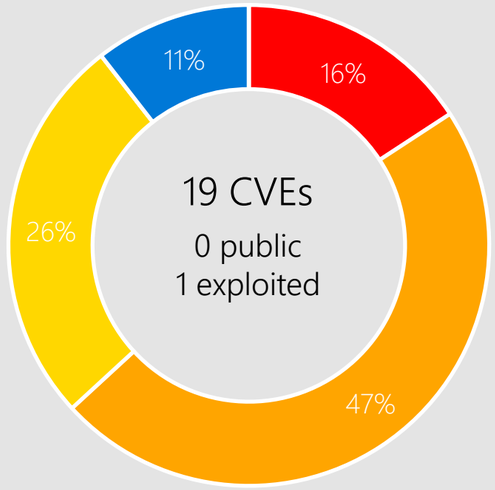
Windows 11, Server 2022



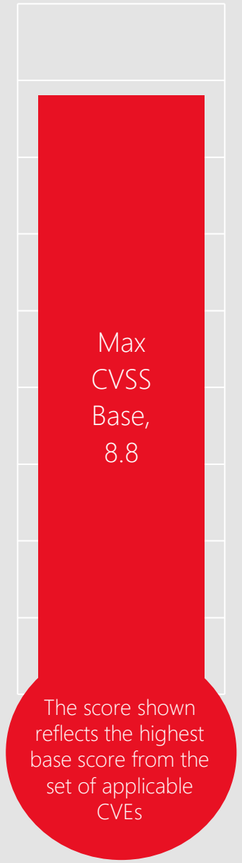
Windows 11 22H2



Windows 11



Windows Server 2022



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

Affected Components:

Cloud Files Mini Filter Driver
Common Log File System Driver
DHCP Server Service
GDI
Internet Connection Sharing (ICS)
Kernel
Miracast Wireless Display
Scripting Engine
Streaming Service Proxy

CVE-2023-38148 Internet Connection Sharing (ICS)

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Exploitation of this vulnerability requires that the Internet Connection Sharing (ICS) is enabled.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-38146 Themes

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.

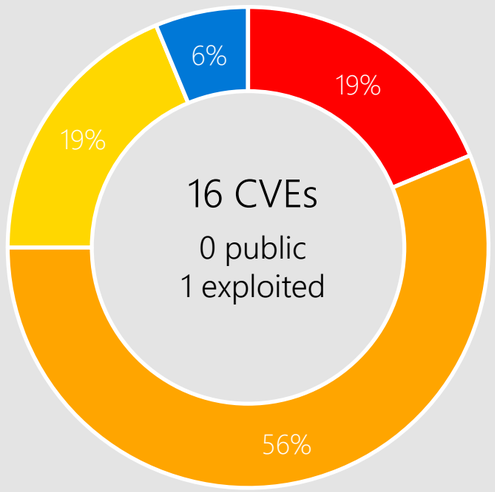
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

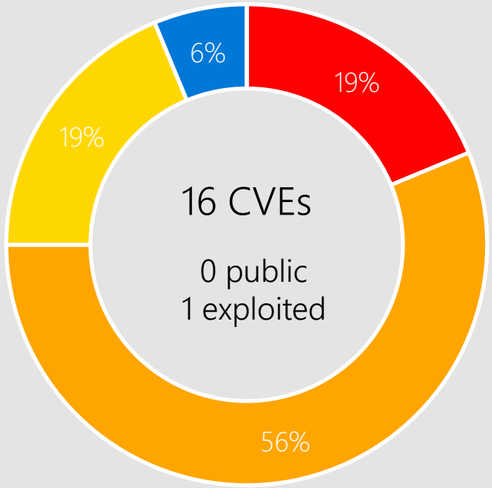
Affected Software

Windows 11 22H2
Windows 11 version 21H2

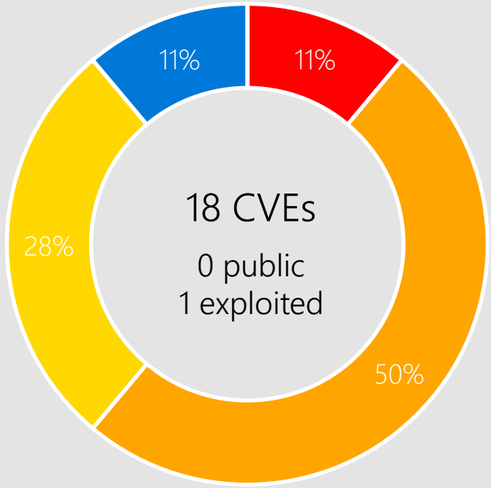
Windows 10



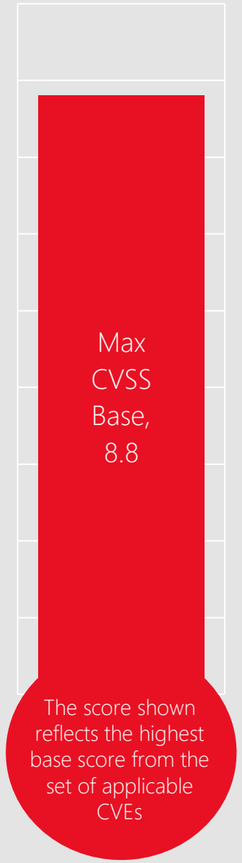
Windows 10 22H2



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:

Cloud Files Mini Filter Driver
Common Log File System Driver
DHCP Server Service
GDI
Kernel
Miracast Wireless Display
Scripting Engine
Streaming Service Proxy
TCP/IP

CVE-2023-36802 Streaming Service Proxy

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation detected

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-38147 Miracast Wireless Display

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

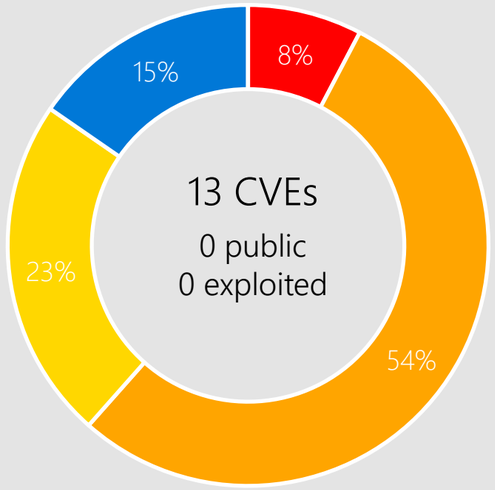
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

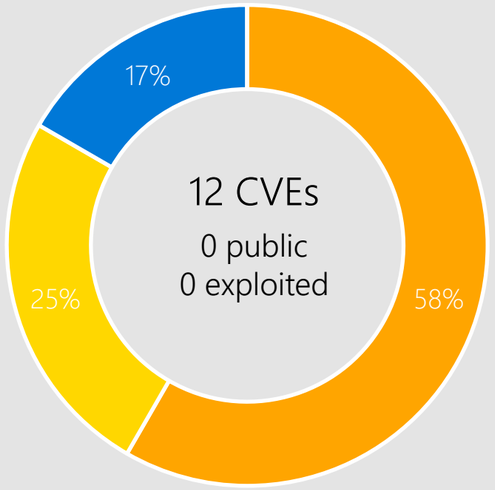
Affected Software

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

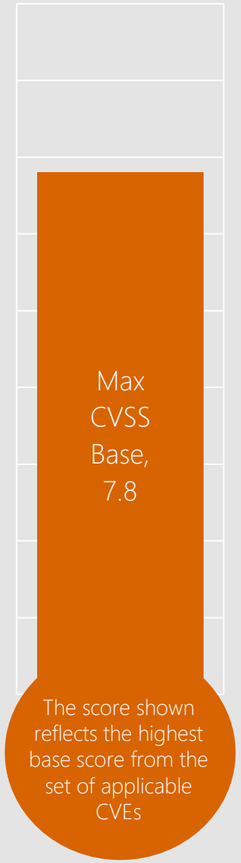
Server 2012 R2, and Server 2012



Server 2012 R2



Windows Server 2012

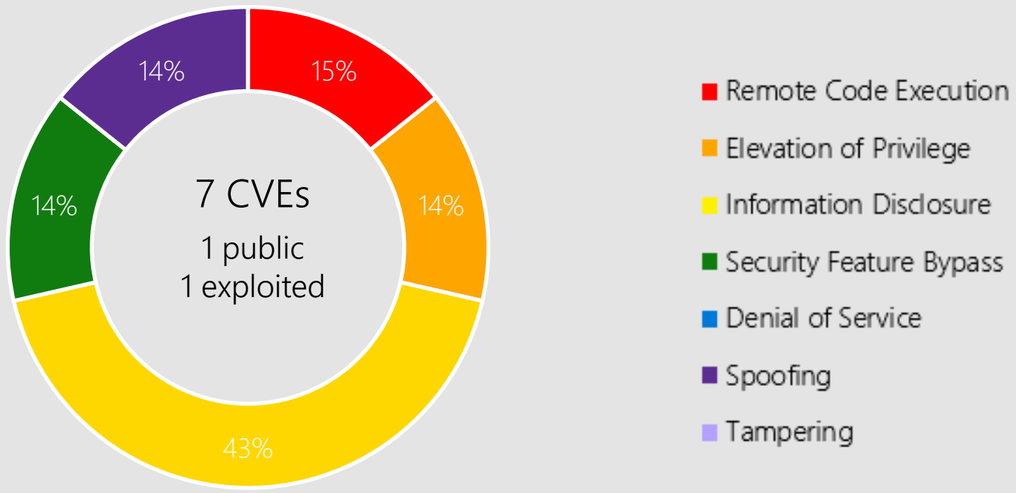


Remote Code Execution Elevation of Privilege Information Disclosure Security Feature Bypass Denial of Service Spoofing Tampering

Affected Components:

Common Log File
System Driver
DHCP Server Service
GDI
Kernel
Scripting Engine
TCP/IP

Microsoft Office



Microsoft Office-related software

Products:

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

CVE-2023-36761 Word

Impact, Severity, Disclosure

Information Disclosure | Important | Publicly Disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 6.2 | 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

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

CVE-2023-36764 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | 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

SharePoint Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

Other Products

Dynamics 365

CVE-2023-36800 | 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 Finance and Operations.

CVE-2023-36886 | 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 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Dynamics 365

CVE-2023-38164 | 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 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Exchange Server

CVE-2023-36744 | 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 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

CVE-2023-36745 | 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 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 13.

Other Products

Exchange Server

CVE-2023-36756 | 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-2023-36757 | 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

Exchange Server

CVE-2023-36777 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.7
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

.NET 6.0 & .NET 7.0

CVE-2023-36792 | 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 6.0, .NET 7.0. Also .NET Framework, Visual Studio

CVE-2023-36793 | 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 6.0, .NET 7.0. Also .NET Framework and Visual Studio

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-36796 | 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 6.0, .NET 7.0. Also .NET Framework and Visual Studio

CVE-2023-36794 | 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 6.0, .NET 7.0. Also .NET Framework and Visual Studio

Other Products

.NET 6.0 & .NET 7.0

CVE-2023-36799 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET 6.0, .NET 7.0. Also Visual Studio

Other Products

.NET Framework

CVE-2023-36788 | 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 AND 4.8.1 on Windows 11 22H2, .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 10 21H2, .NET Framework 2.0 on Server 2008, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.0 on Server 2008, .NET Framework 3.5 on Server 2012, .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 Windows 10 1809, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.7.2 on Server 2019.

Other Products

.NET Framework

CVE-2023-36792 | 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 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 2008 R2, .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 4.8 on Windows 10 22H2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .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 4.8.1 on Windows 11 version 21H2, .NET Framework 3.0 on Server 2008, .NET Framework 2.0 on Server 2008, .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 11 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 21H2, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 3.5.1 on Server 2008 R2, .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 Windows 10 21H2, .NET Framework 4.8 on Server 2012, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 4.8 on Windows 10 1607, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2008 R2, .NET Framework 4.8 on Server 2016. Also Visual Studio, .NET 6.0, .NET 7.0.

Other Products

.NET Framework

CVE-2023-36793 | 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 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 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .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 4.8.1 on Windows 10 21H2, .NET Framework 3.0 on Server 2008, .NET Framework 2.0 on Server 2008, .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 version 21H2, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2016, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 4.8 on Windows 10 1607, .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 4.8 on Server 2008 R2, .NET Framework 4.8 on Server 2012 R2. Also Visual Studio, .NET 6.0, .NET 7.0.

Other Products

.NET Framework

CVE-2023-36794 | 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 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 4.8.1 on Windows 10 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 3.5 on Server 2012, .NET Framework 2.0 on Server 2008, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.0 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 4.8 on Server 2012 R2, .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 Windows 10 1607, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.5 AND 4.8 on Windows 10 22H2, .NET Framework 4.8 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2. Also Visual Studio, .NET 6.0, .NET 7.0.

Other Products

.NET Framework

CVE-2023-36796 | 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 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 2008 R2, .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 AND 4.8 on Windows 10 22H2, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 AND 4.7.2 on Windows 10 1809, .NET Framework 3.5 AND 4.8 on Windows 10 21H2, .NET Framework 3.0 on Server 2008, .NET Framework 2.0 on Server 2008, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 on Server 2012, .NET Framework 4.6.2 on Server 2008, .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 4.8.1 on Windows 11 22H2, .NET Framework 3.5 AND 4.8.1 on Windows 10 22H2, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Server 2016, .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 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 4.8 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 10 1809, .NET Framework 4.8 on Server 2012 R2. Also Visual Studio, .NET 6.0, .NET 7.0.

Other Products

Visual Studio

CVE-2023-36792 | 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 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.7, Visual Studio 2015 Update 3, Visual Studio 2013 Update 5. Also .NET Framework, .NET 6.0, .NET 7.0.

CVE-2023-36793 | 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 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2013 Update 5, Visual Studio 2022 version 17.7, Visual Studio 2022 version 17.6, Visual Studio 2015 Update 3. Also .NET Framework, .NET 6.0, .NET 7.0

Other Products

Visual Studio

CVE-2023-36796 | 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 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.7, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2015 Update 3, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2013 Update 5. Also .NET Framework, .NET 6.0, .NET 7.0.

CVE-2023-36742 | 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 Code.

Other Products

Visual Studio

CVE-2023-36794 | 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 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2013 Update 5, Visual Studio 2022 version 17.7, Visual Studio 2022 version 17.6, Visual Studio 2015 Update 3. Also .NET Framework, .NET 6.0, .NET 7.0.

CVE-2023-36758 | 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: Visual Studio 2022 version 17.7.

Other Products

Visual Studio

CVE-2023-36759 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.7
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.7, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-36799 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.7, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, .NET 6.0, .NET 7.0.

Other Products

Visual Studio

CVE-2023-39956 | Important | Remote Code Execution | Public: No | Exploited: No

CVE details: https://www.cve.org/CVERecord?id=CVE-2023-39956

Products: Visual Studio Code

Other Products

Azure DevOps Server

CVE-2023-33136 | 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: Azure DevOps Server 2022.0.1, Azure DevOps Server 2020.0.2, Azure DevOps Server 2019.1.2, Azure DevOps Server 2020.1.2, Azure DevOps Server 2019.0.1.

CVE-2023-38155 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Azure DevOps Server 2022.0.1, Azure DevOps Server 2020.0.2, Azure DevOps Server 2019.1.2, Azure DevOps Server 2020.1.2, Azure DevOps Server 2019.0.1.

Other Products

Azure HDInsights

CVE-2023-38156 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Azure HDInsights.

Other Products

Azure Kubernetes Service

CVE-2023-29332 | Critical | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure Kubernetes Service.

Other Products

Windows Defender

CVE-2023-38163 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Microsoft Defender Security Intelligence Updates

Other Products

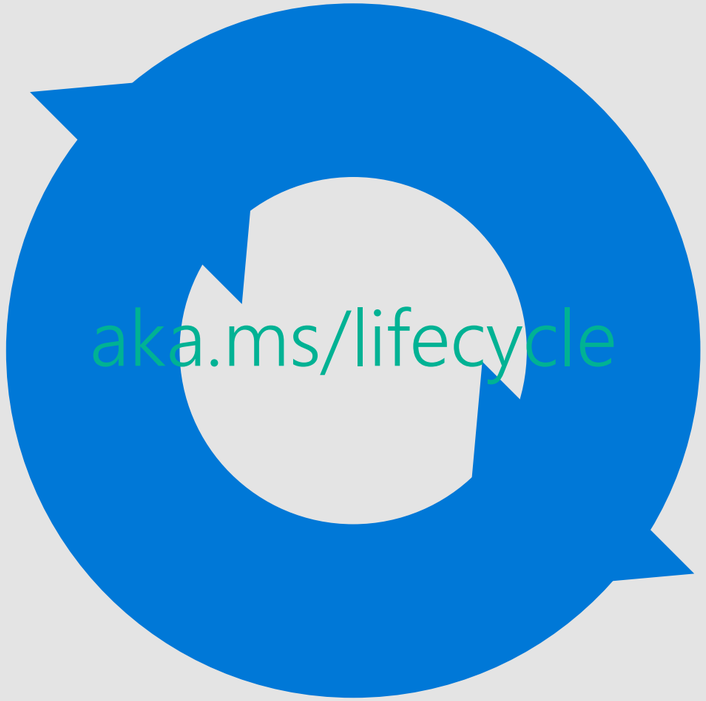
Apps and Identity

CVE-2023-36736 Microsoft Identity Linux Broker
CVE-2023-36772/36773/36770/36771 3D Builder
CVE-2022-41303/CVE-2023-36739/36740/36760 3D Viewer

Product Lifecycle Update

Nothing reaching end of support in September

October 2023 Windows Server 2012 and 2012 R2 will reach end of support



Overview of Windows Server Upgrades

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-35355	No	No	Cloud Files Mini Filter Driver
CVE-2023-38162	No	No	DHCP Server Service
CVE-2023-38161	No	No	GDI
CVE-2023-38152	No	No	DHCP Server Service
CVE-2023-38150	No	No	Kernel
CVE-2023-38149	No	No	TCP/IP
CVE-2023-38148	No	No	Internet Connection Sharing (ICS)
CVE-2023-38147	No	No	Miracast Wireless Display
CVE-2023-38146	No	No	Themes
CVE-2023-38144	No	No	CLFS Driver
CVE-2023-38143	No	No	CLFS Driver
CVE-2023-38142	No	No	Kernel
CVE-2023-38141	No	No	Kernel
CVE-2023-38140	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-38139	No	No	Kernel
CVE-2023-36805	No	No	Scripting Engine
CVE-2023-36804	No	No	GDI
CVE-2023-36803	No	No	Kernel
CVE-2023-36801	No	No	DHCP Server Service
CVE-2023-38163	No	No	Defender Attack Surface Reduction
CVE-2023-38160	No	No	TCP/IP
CVE-2023-36767	No	No	Office
CVE-2023-36766	No	No	Excel
CVE-2023-36765	No	No	Office

CVE	Public	Exploited	Product
CVE-2023-41764	No	No	Office
CVE-2023-36764	No	No	SharePoint Server
CVE-2023-36763	No	No	Outlook
CVE-2023-36762	No	No	Word
CVE-2023-36761	Yes	Yes	Word
CVE-2023-38156	No	No	Azure HDInsight Apache Ambari
CVE-2023-36802	No	No	Streaming Service Proxy
CVE-2023-36759	No	No	Visual Studio
CVE-2023-36758	No	No	Visual Studio
CVE-2023-36757	No	No	Exchange Server
CVE-2023-36756	No	No	Exchange Server
CVE-2023-36745	No	No	Exchange Server
CVE-2023-36744	No	No	Exchange Server
CVE-2023-36742	No	No	Visual Studio Code

CVE	Public	Exploited	Product
CVE-2023-36736	No	No	Identity Linux Broker
CVE-2022-41303	No	No	AutoDesk
CVE-2023-29332	No	No	Azure Kubernetes Service
CVE-2023-33136	No	No	Azure DevOps Server
CVE-2023-36886	No	No	Dynamics 365
CVE-2023-38164	No	No	Dynamics 365
CVE-2023-38155	No	No	Azure DevOps Server and Team Foundation Server
CVE-2023-36800	No	No	Dynamics Finance and Operations
CVE-2023-36799	No	No	.NET Core and Visual Studio
CVE-2023-36796	No	No	Visual Studio
CVE-2023-36794	No	No	Visual Studio
CVE-2023-36793	No	No	Visual Studio
CVE-2023-36792	No	No	Visual Studio
CVE-2023-36788	No	No	.NET Framework

CVE	Public	Exploited	Product
CVE-2023-36777	No	No	Exchange Server
CVE-2023-36773	No	No	3D Builder
CVE-2023-36772	No	No	3D Builder
CVE-2023-36771	No	No	3D Builder
CVE-2023-36770	No	No	3D Builder
CVE-2023-36760	No	No	3D Viewer
CVE-2023-39956	No	No	Electron: CVE-2023-39956 -Visual Studio Code
CVE-2023-36740	No	No	3D Viewer
CVE-2023-36739	No	No	3D Viewer