Microsoft

Microsoft Security Release

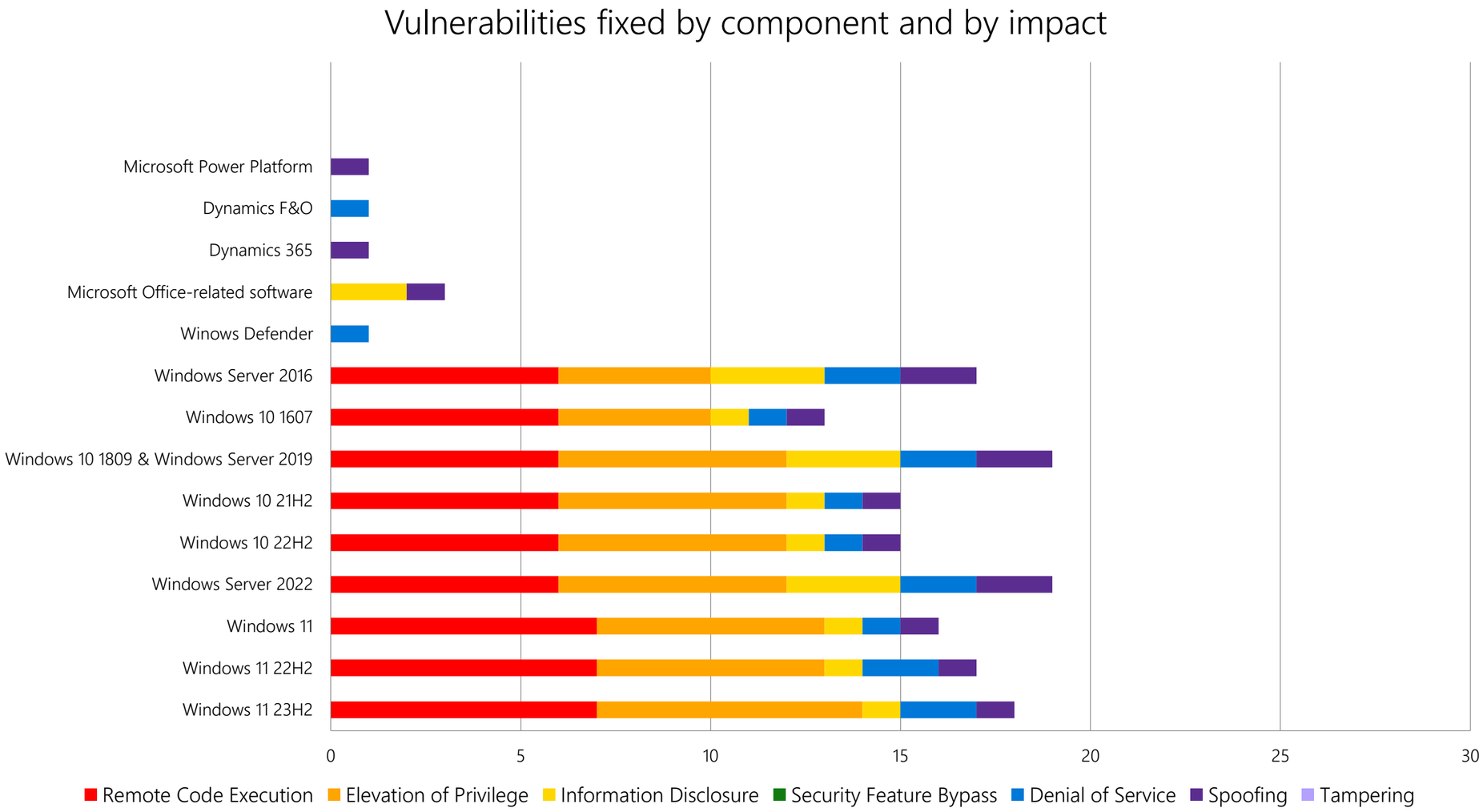
December 12, 2023

Agenda

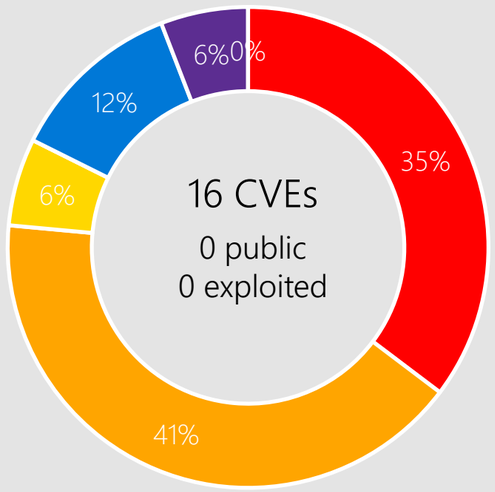
Security Updates

Product Support Lifecyle

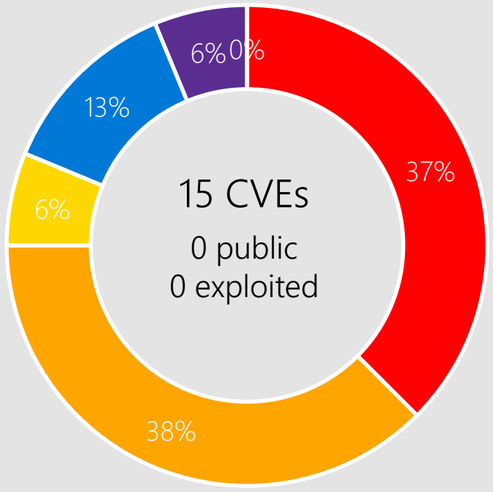
Monthly Security Release Overview - December 2023



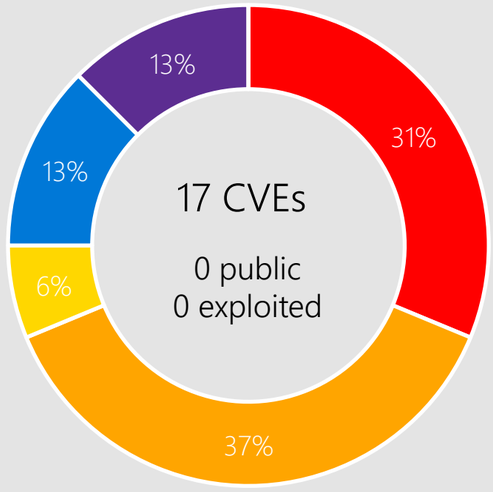
Windows 11, Server 2022



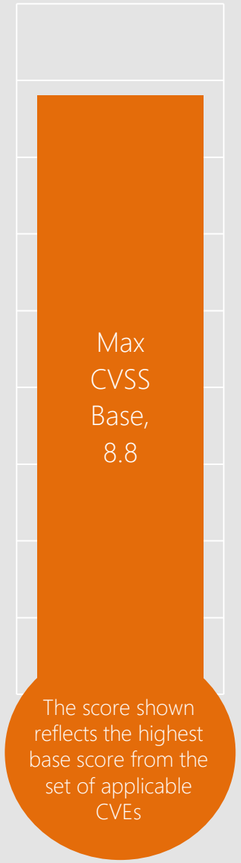
Windows 11 23H2



Windows 11 22H2



Windows Server 2022 23H2



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

Affected Components:

See Appendix for details

CVE-2023-35641 Internet Connection Sharing

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

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-2023-35639 Windows ODBC Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11
- Windows 10
- Server 2022
- Server 2019
- Server 2016

CVE-2023-35634 Microsoft Bluetooth Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.0 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

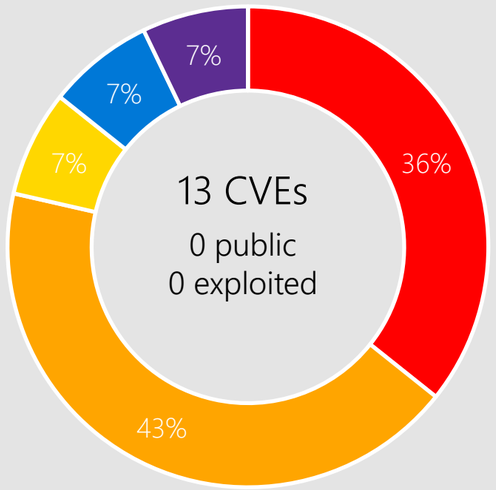
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

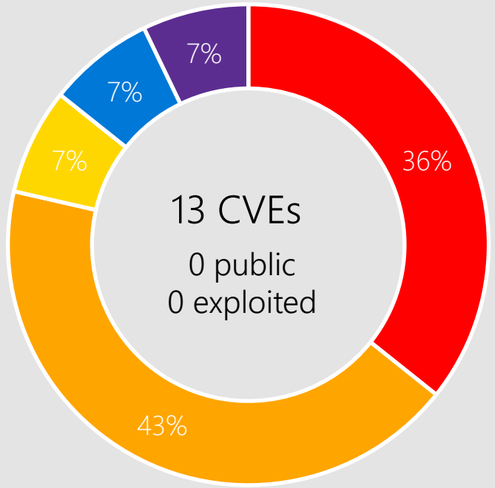
Affected Software

Windows 11

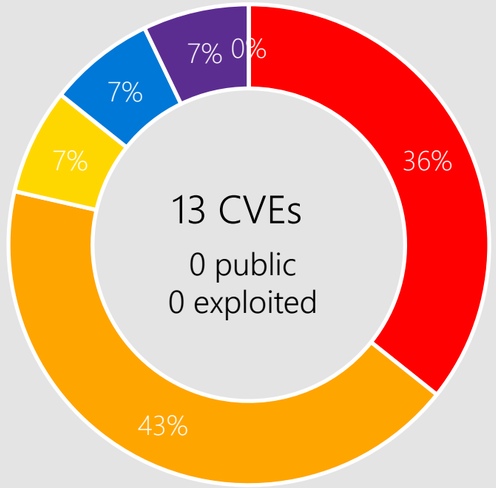
Windows 10



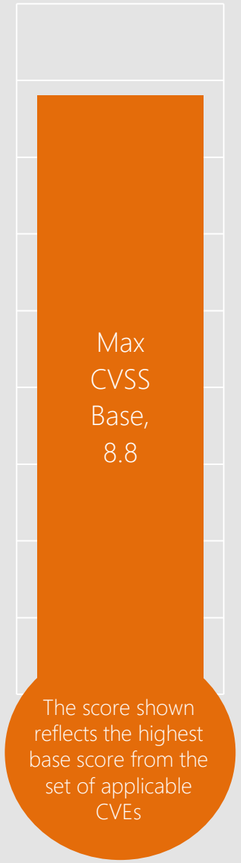
Windows 10 22H2



Windows 10 21H2



Windows 10 1809 & 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-2023-36006 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-2023-35628 MSHTML Platform

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

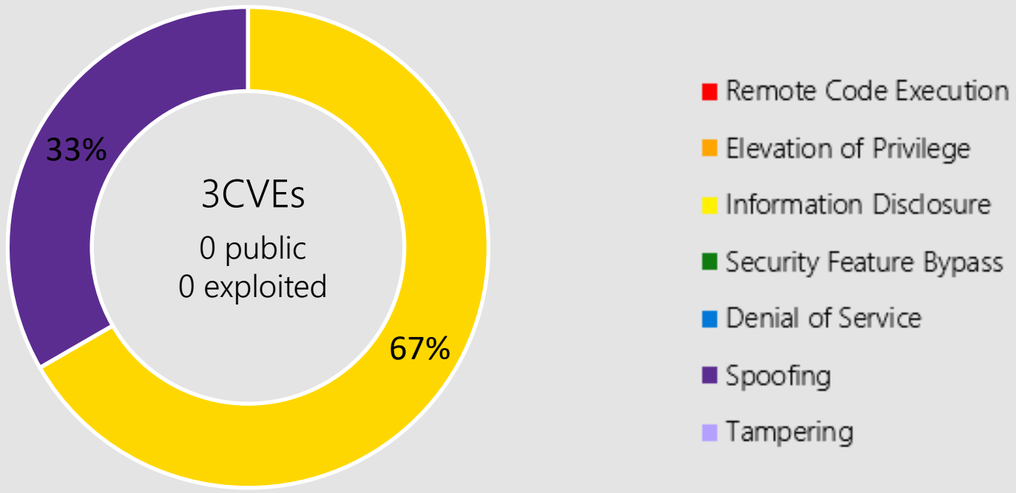
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11
- Windows 10
- Server 2022
- Server 2019
- Server 2016

Microsoft Office



Microsoft Office-related software

Products:

Microsoft 365 Apps for Enterprise
Microsoft Office LTSC for Mac 2021
Microsoft Office 2016
Microsoft Office 2019
Microsoft Office LTSC 2021

CVE-2023-35636 Outlook

Impact, Severity, Disclosure

Information Disclosure | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 6.5 | 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

365 Apps for Enterprise
Office 2016
Office 2019
Office LTSC 2021

Other Products

Dynamics 365

CVE-2023-36020 | 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 9.0,9.1.

CVE-2023-35621 | 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: Dynamics 365 for Finance and Operations platform update 60, Dynamics 365 for Finance and Operations version 10.0.37 platform update 61, Dynamics 365 for Finance and Operations version 10.0.38 platform update 62

Other Products

Microsoft Power Platform

CVE-2023-36019 | Critical | Spoofing | Public: No | Exploited: No

CVSS Base Score: 9.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Azure Logic Apps, Microsoft Power Platform

Other Products

Windows Defender

CVE-2023-36010 | 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: Microsoft Malware Protection Platform

Other Products

Azure

CVE-2023-35624 Azure Connected Machine Agent
CVE-2023-35625 Azure Machine Learning SDK

Product Lifecycle Update

No Products Reaching End Of Support in December

aka.ms/lifecycle

HAPPY HOLIDAYS

Microsoft

Questions?

Appendix

Component Name	CVE count
DHCP Server Service	3
Internet Connection Sharing (ICS)	3
Kernel	2
Win32k	2
Ancillary Function Driver for WinSock	1
Bluetooth Driver	1
Cloud Files Mini Filter Driver	1
Defender	1
DNS	1
DPAPI (Data Protection Application Programming Interface)	1
Dynamics 365 (on-premises) Cross-site Scripting	1
Dynamics 365 Finance and Operations	1
MSHTML Platform	1
ODBC Driver	1
Outlook	1
Outlook for Mac	1
Power Platform Connector	1
Sysmain Service	1
Telephony Server	1
USBHUB 3.0 Device Driver	1
WDAC OLE DB provider for SQL Server	1
Word	1
Azure Connected Machine Agent	1
Azure Machine Learning Compute Instance for SDK Users	1
Local Security Authority Subsystem Service	1
XAML Diagnostics	1