Microsoft

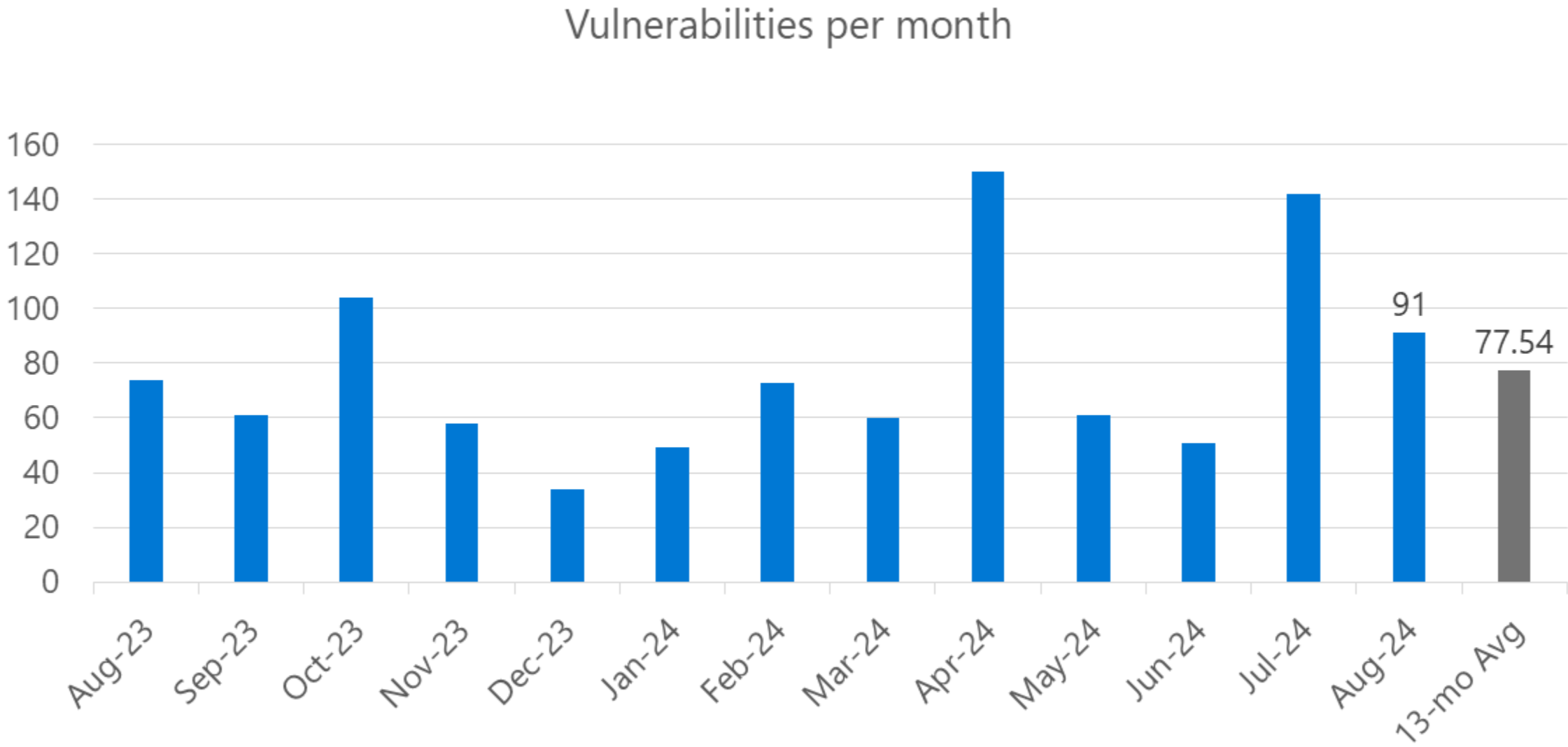
Microsoft Security Release

August 13, 2024

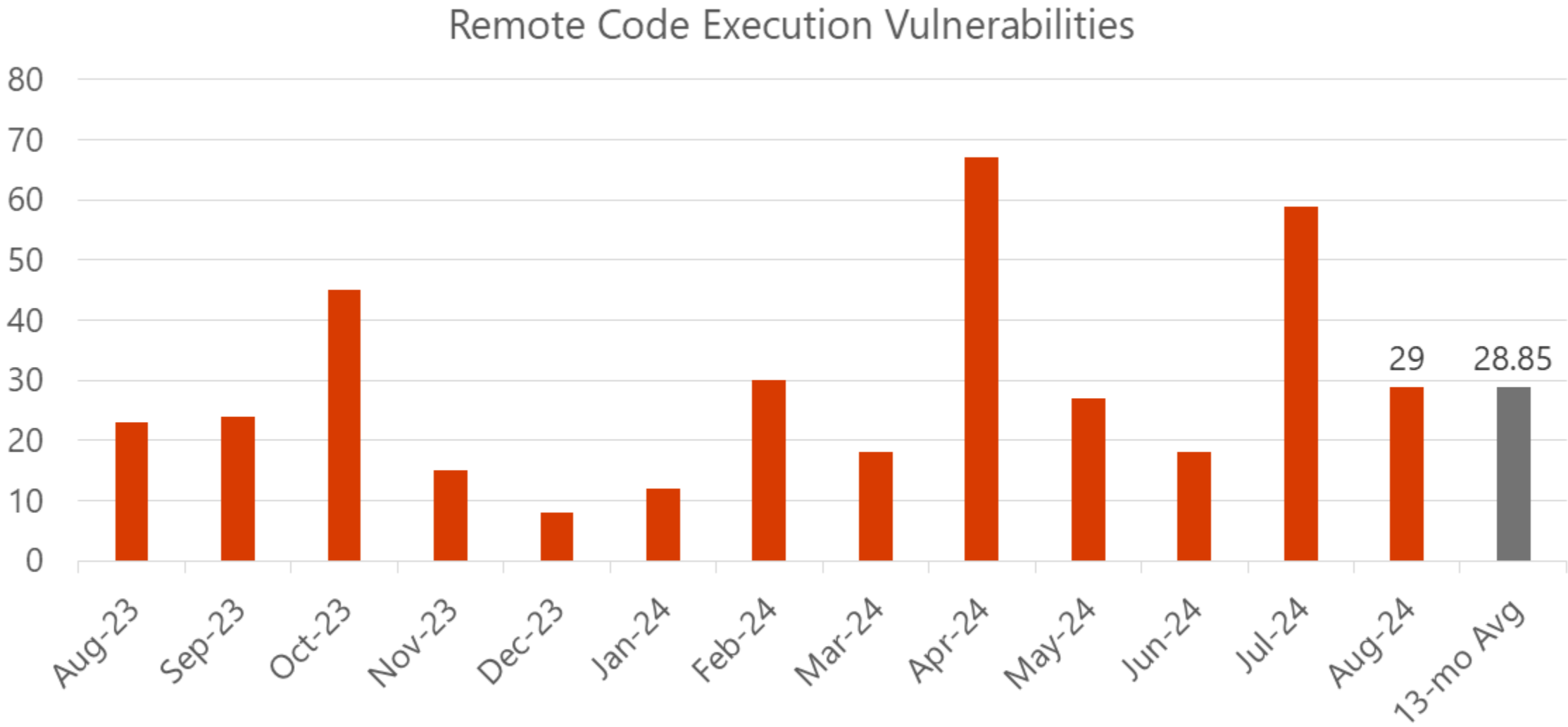
Agenda

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

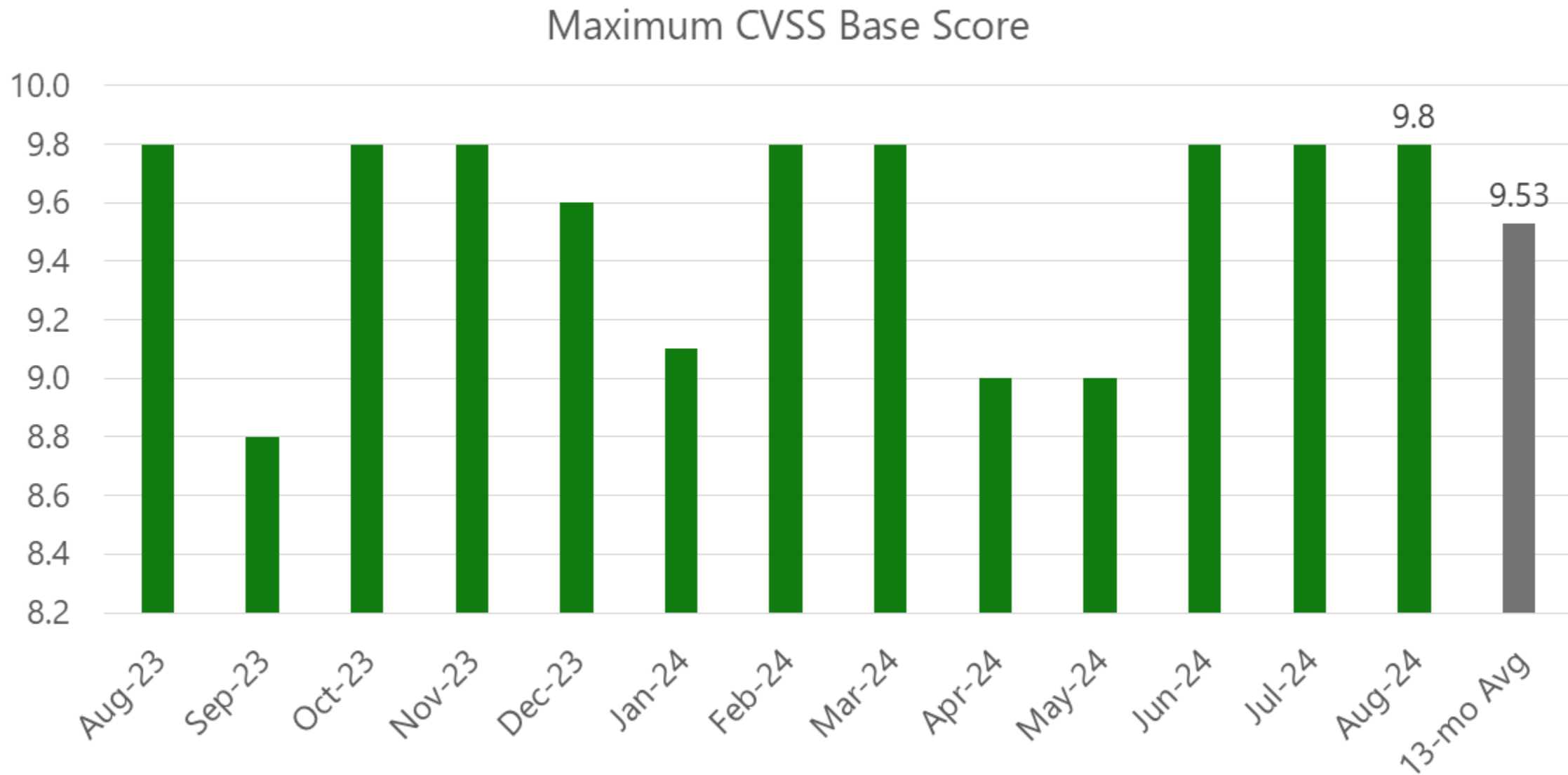
Microsoft


Vulnerabilities per month
160
140
120
100
80
60
40
20
0
91
77.54
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

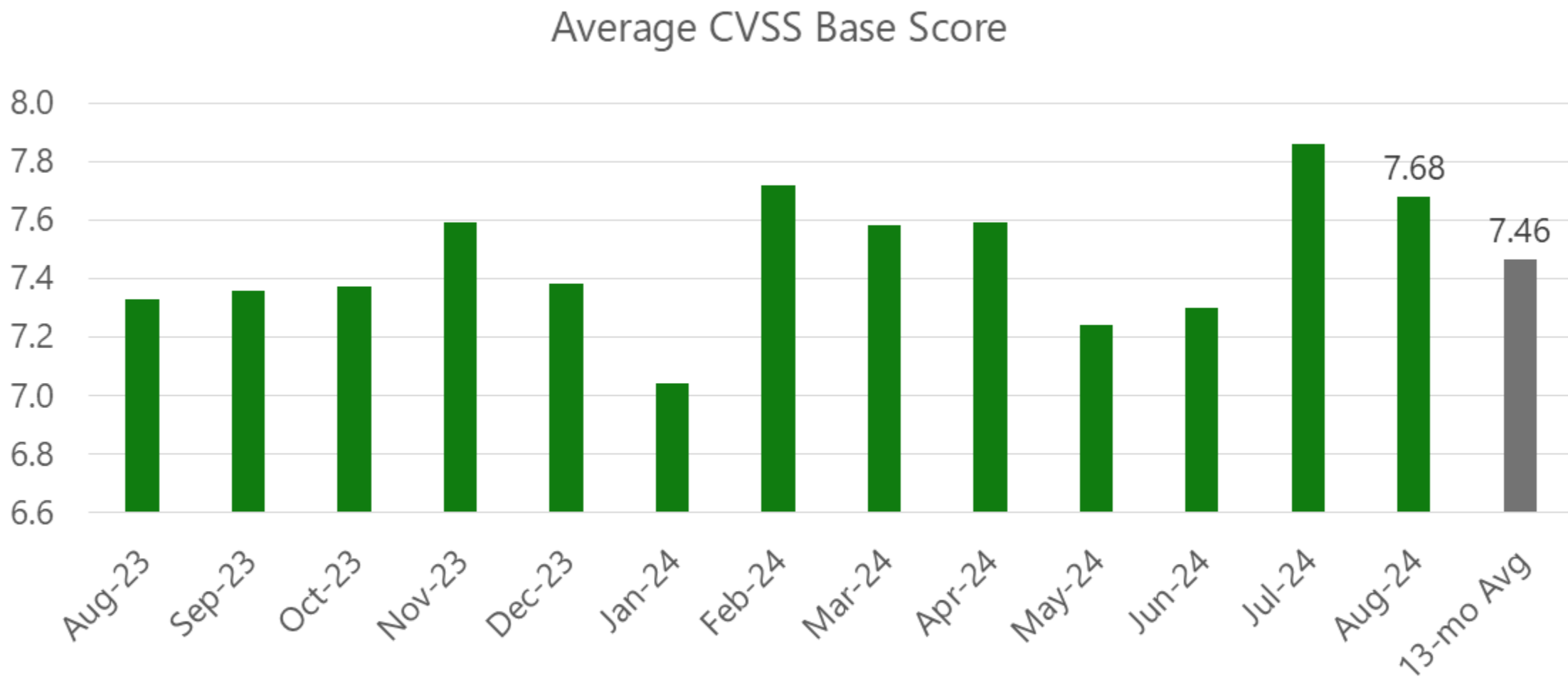
Microsoft


Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
29
28.85
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

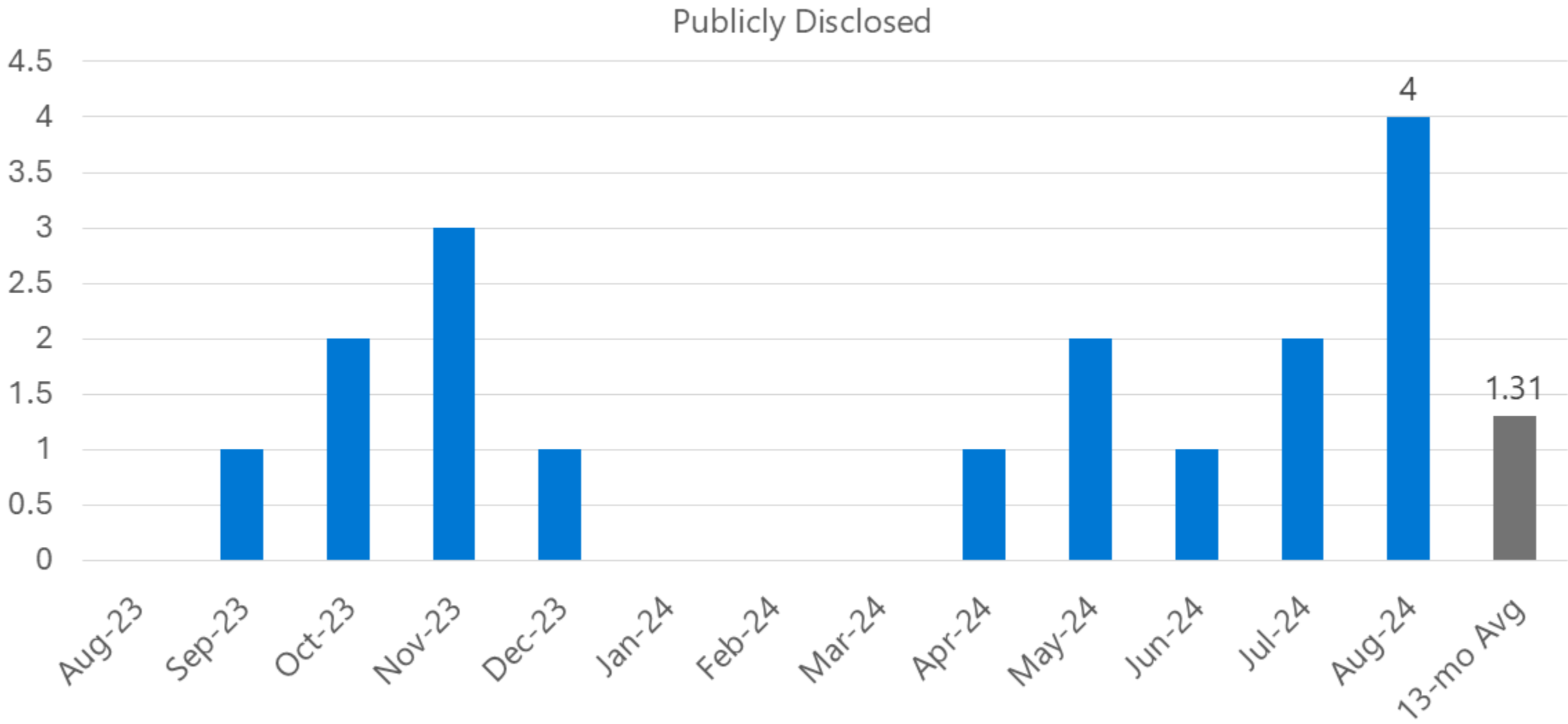
Microsoft


Maximum CVSS Base Score
10.0
9.8
9.6
9.4
9.2
9.0
8.8
8.6
8.4
8.2
9.8
9.53
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

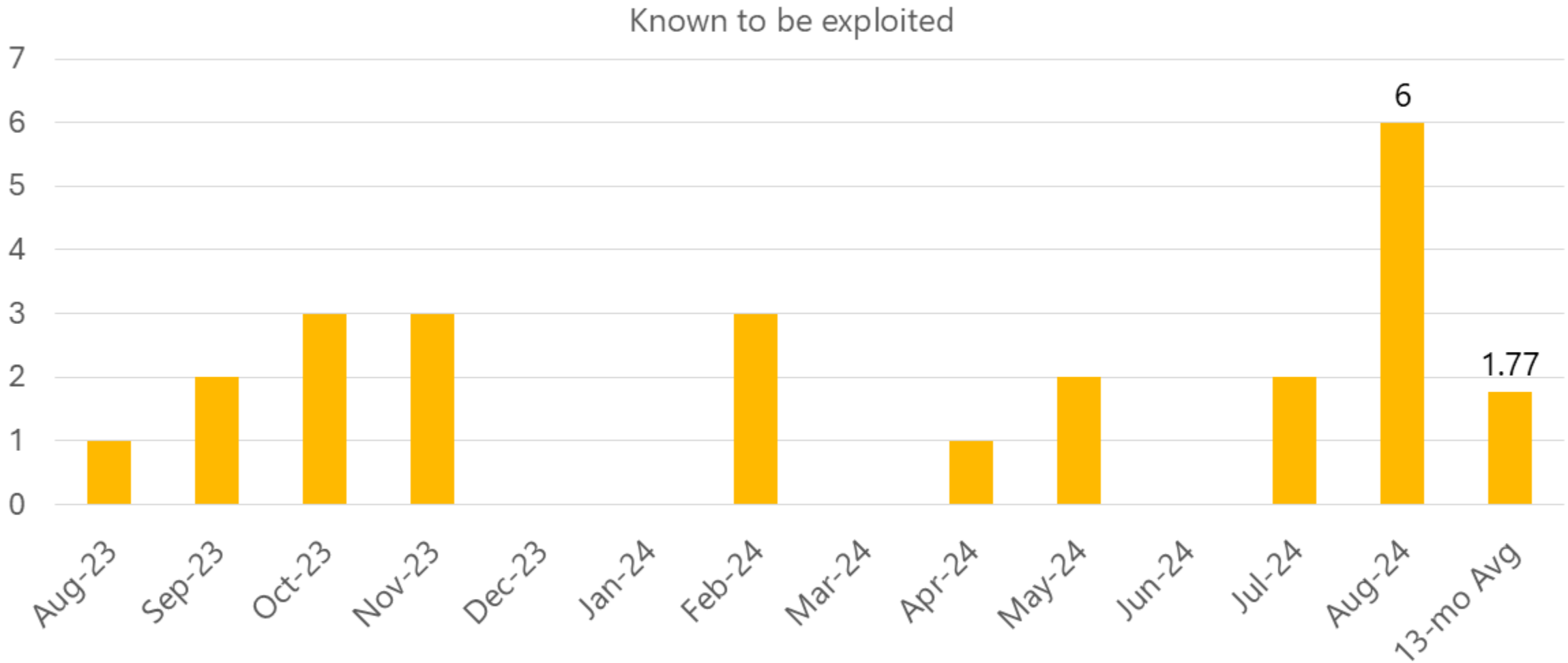
Microsoft


Average CVSS Base Score
8.0
7.8
7.6
7.4
7.2
7.0
6.8
6.6
7.68
7.46
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

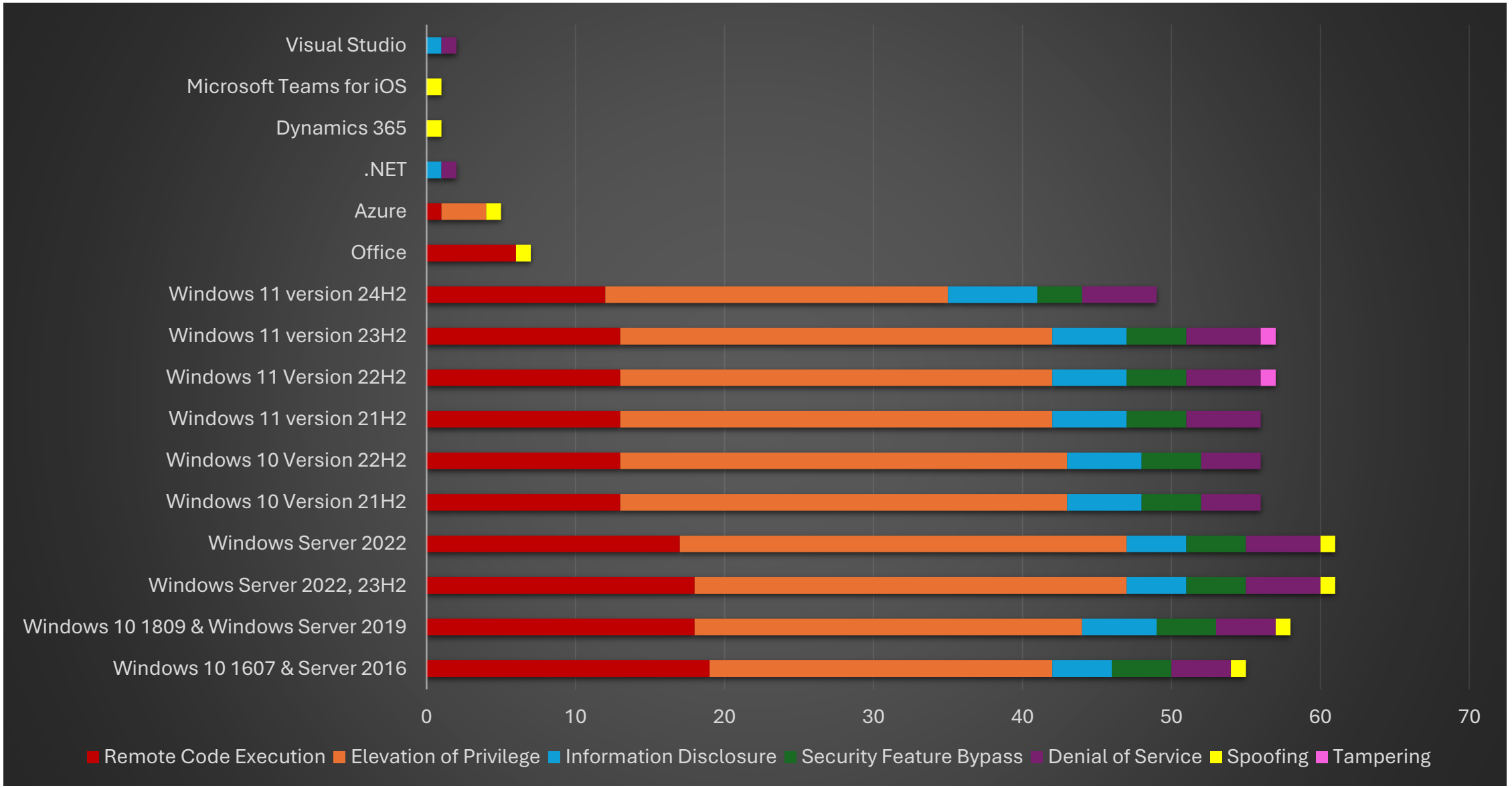
Microsoft


Publicly Disclosed
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
4
1.31
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

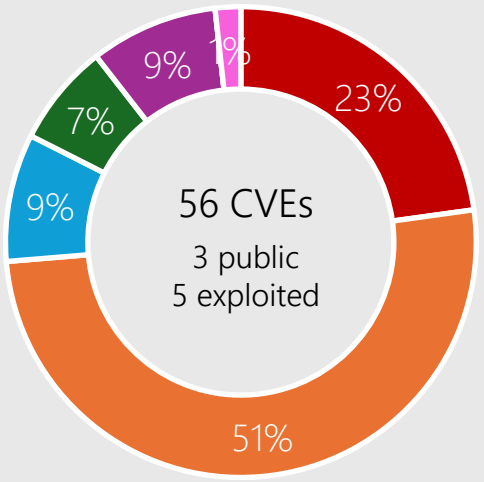
Microsoft


Known to be exploited
7
6
5
4
3
2
1
0
6
1.77
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
13-mo Avg

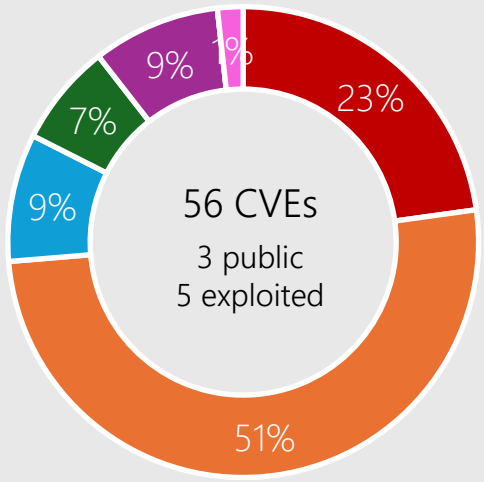
Microsoft Security Release Overview – August 2024



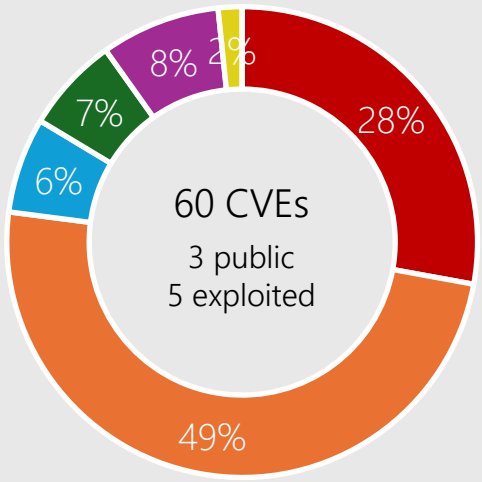
Windows 11, Server 2022



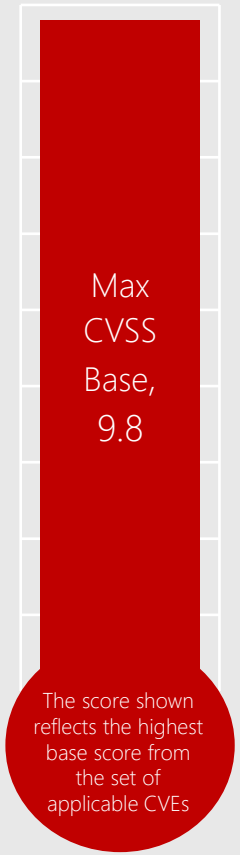
Windows 11 23H2



Windows 11 22H2



Windows Server 2022



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

Affected Components:

See Appendix for details

CVE-2024-38199 Line Printer Daemon

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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

Users are advised against installing or enabling the Line Printer Daemon (LPD) service.
The LPD is not installed or enabled on the systems by default.
The LPD has been announced as deprecated since Windows Server 2012. Please refer to: Features Removed or Deprecated in Windows Server 2012.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38063 TCP/IP

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

Systems are not affected if IPv6 is disabled on the target machine.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38140 RMCAST Driver

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

This vulnerability is only exploitable only if there is a program listening on a Pragmatic General Multicast (PGM) port. If PGM is installed or enabled but no programs are actively listening as a receiver, then this vulnerability is not exploitable.

PGM does not authenticate requests, so it is recommended to protect access to any open ports at the network level (e.g. with a firewall). It is not recommended to expose a PGM receiver to the public internet.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38193 Ancillary Function Driver

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
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38107 Power Dependency Coord.

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.

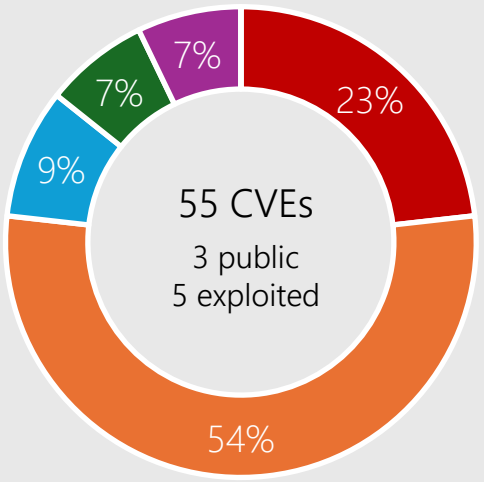
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

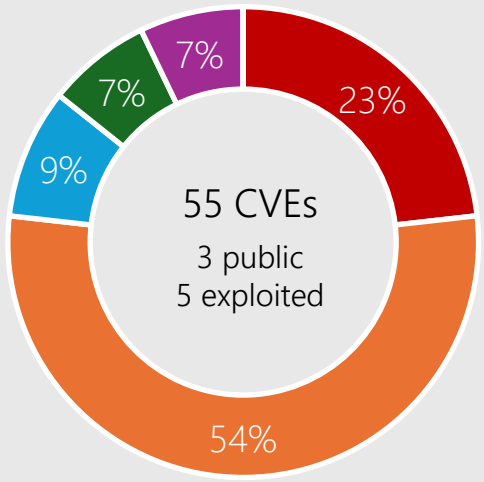
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

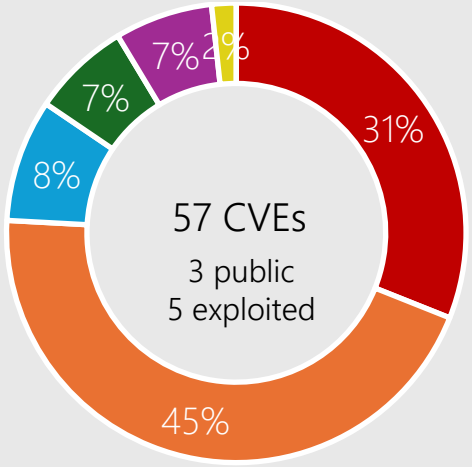
Windows 10



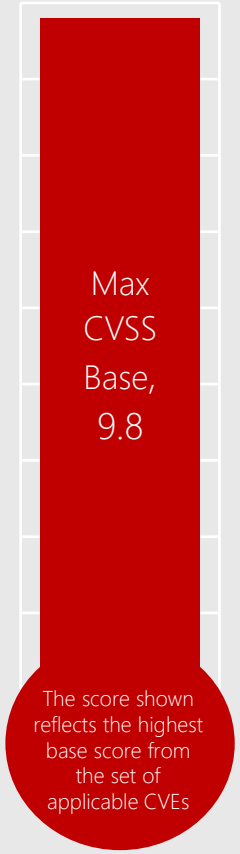
Windows 10 22H2



Windows 10 21H2



Windows 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-2024-38159 Network Virtualization

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.1 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | User Interaction: None

Mitigations

Ensuring that the virtual machine (VM) is running on the VMware hypervisor exclusively, as it needs to be capable of nested virtualization.
Disabling Hyper-V and its dependent features (VBS and its components) on the host where the VM will run is also crucial.
Renaming the hypervisor binary (C:\Windows\System32\hvix64.exe) to prevent it from loading at boot time can also help mitigate the issue.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 10 v1607
Server 2016

CVE-2024-38178 Scripting Engine

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38106 Kernel

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 7.0 | Attack Vector: Local | Attack Complexity: High | 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
Server 2022
Server 2019
Server 2016

CVE-2024-21302 Secure Kernel Mode

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 6.7 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: High | User Interaction: None

Mitigations

In addition to applying the August 2024 updates, apply the opt-in policy documented here: KB5042562: Guidance for blocking rollback of virtualization-based security related updates.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

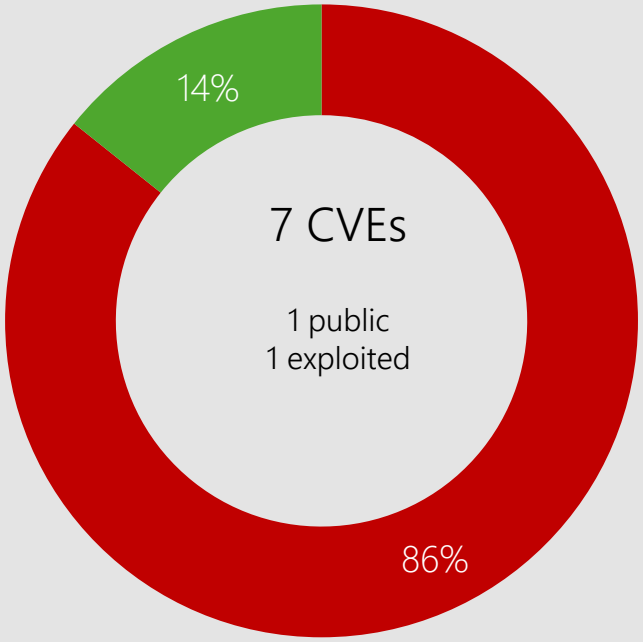
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Windows CVEs: CVSS 8.8

- CVE-2024-38114 IP Routing Management Snapin
- CVE-2024-38120 RRAS (Routing and Remote Access)
- CVE-2024-38131 Clipboard Virtual Channel Extension
- CVE-2024-38144 Kernel Streaming WOW Thunk Service Driver
- CVE-2024-38180 SmartScreen Prompt

Microsoft Office



Microsoft Office-related software

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

Products:

Office 2016
Office 2019
Outlook 2016
Project 2016
PowerPoint 2016
365 Apps Enterprise
Office LTSC 2021
Office LTSC for Mac 2021

CVE-2024-38189 Project

Impact, Severity, Disclosure

Remote Code Execution | 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 strongly recommends customers do not disable the Block macros from running in Office files from the Internet policy which protects against this vulnerability. However, customers who have disabled this policy can alternatively enable VBA Macro Notification Settings to protect their systems from this vulnerability being exploited.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Project 2016
Office 2019
Office 365 Apps for Enterprise
Office LTSC 2021

CVE-2024-38172 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 365 Apps for Enterprise
Office LTSC for Mac 2021

CVE-2024-38200 Office

Impact, Severity, Disclosure

Spoofing | Important | Publicly 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

Add users to the Protected Users Security Group, which prevents the use of NTLM as an authentication mechanism
Block TCP 445/SMB outbound
Restrict outgoing NTLM traffic to remote servers. See CVE entry for details

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

Other Products

Dynamics 365

CVE-2024-38211 | Important | Spoofing | Public: No | Exploited: No

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

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-38168 | .NET and Visual Studio Denial of ServiceVulnerability

Base CVSS: 7.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: .NET 8.0, Visual Studio 2022

CVE-2024-38167 | .NET and Visual Studio Information Disclosure

Base CVSS: 6.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: Yes
Affected Products: .NET 8.0, Visual Studio 2022

Other Products

Azure, Apps

CVE-2024-38158 C SDK for Azure IoT
CVE-2024-38157 Azure IoT Hub Device Client SDK
CVE-2024-38109 Azure Health Bot
CVE-2024-38195 Azure Cycle Cloud
CVE-2024-38162/38098 Azure connected Machine Agent
CVE-2024-38201/38108 Azure Stack Hub
CVE-2024-38177 Windows App Installer
CVE-2024-38197 Teams for iOS

Product Lifecycle Update

Products reaching end of support

Azure Kinect SDK
Visual Studio for Mac

Microsoft

Questions?

Appendix

CVE	Component	Public	Exploited
CVE-2024-21302 Windows Secure Kernel Mode	Secure Kernel Mode	Yes	No
CVE-2024-29995 Windows Kerberos	Kerberos	No	No
CVE-2024-37968 Microsoft Windows DNS	DNS	No	No
CVE-2024-38063 Windows TCP/IP	TCP/IP	No	No
CVE-2024-38084 Microsoft Office	OfficePlus	No	No
CVE-2024-38098 Azure Connected Machine Agent	Azure Connected Machine Agent	No	No
CVE-2024-38106 Windows Kernel	Kernel	No	Yes
CVE-2024-38107 Windows Power Dependency Coordinator	Power Dependency Coordinator	No	Yes
CVE-2024-38108 Azure Stack	Azure Stack Hub	No	No
CVE-2024-38109 Azure Health Bot	Azure Health Bot	No	No
CVE-2024-38114 Windows IP Routing Management Snapin	IP Routing Management Snapin	No	No
CVE-2024-38115 Windows IP Routing Management Snapin	IP Routing Management Snapin	No	No
CVE-2024-38116 Windows IP Routing Management Snapin	IP Routing Management Snapin	No	No
CVE-2024-38117 Windows NTFS	NTFS	No	No
CVE-2024-38118 Microsoft Local Security Authority Server (lsasrv)	Local Security Authority (LSA) Server	No	No
CVE-2024-38120 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38121 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No

CVE	Component	Public	Exploited
CVE-2024-38122 Microsoft Local Security Authority Server (lsasrv)	Local Security Authority (LSA) Server	No	No
CVE-2024-38123 Microsoft Bluetooth Driver	Bluetooth Driver	No	No
CVE-2024-38125 Microsoft Streaming Service	Kernel Streaming WOW Thunk Service Driver	No	No
CVE-2024-38126 Windows Network Address Translation (NAT)	Network Address Translation (NAT)	No	No
CVE-2024-38127 Windows Kernel	Hyper-V	No	No
CVE-2024-38128 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38130 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38131 Windows Clipboard Virtual Channel Extension	Clipboard Virtual Channel Extension	No	No
CVE-2024-38132 Windows Network Address Translation (NAT)	Network Address Translation (NAT)	No	No
CVE-2024-38133 Windows Kernel	Kernel	No	No
CVE-2024-38134 Microsoft Streaming Service	Kernel Streaming WOW Thunk Service Driver	No	No
CVE-2024-38135 Windows NT OS Kernel	Resilient File System (ReFS)	No	No
CVE-2024-38136 Windows Resource Manager	Resource Manager PSM Service Extension	No	No
CVE-2024-38137 Windows Resource Manager	Resource Manager PSM Service Extension	No	No
CVE-2024-38138 Windows Deployment Services	Deployment Services	No	No
CVE-2024-38140 Reliable Multicast Transport Driver (RMCAST)	Reliable Multicast Transport Driver (RMCAST)	No	No
CVE-2024-38141 Windows Ancillary Function Driver for WinSock	Ancillary Function Driver for WinSock	No	No

CVE	Component	Public	Exploited
CVE-2024-38142 Windows Secure Kernel Mode	Secure Kernel Mode	No	No
CVE-2024-38143 Windows WLAN Auto Config Service	WLAN AutoConfig Service	No	No
CVE-2024-38144 Microsoft Streaming Service	Kernel Streaming WOW Thunk Service Driver	No	No
CVE-2024-38145 Windows Layer-2 Bridge Network Driver	Layer-2 Bridge Network Driver	No	No
CVE-2024-38146 Windows Layer-2 Bridge Network Driver	Layer-2 Bridge Network Driver	No	No
CVE-2024-38147 Windows DWM Core Library	DWM Core Library	No	No
CVE-2024-38148 Windows Transport Security Layer (TLS)	Secure Channel	No	No
CVE-2024-38150 Windows DWM Core Library	DWM Core Library	No	No
CVE-2024-38151 Windows Kernel	Kernel	No	No
CVE-2024-38152 Microsoft WDAC OLE DB provider for SQL	OLE	No	No
CVE-2024-38153 Windows Kernel	Kernel	No	No
CVE-2024-38154 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38155 Windows Security Center	Security Center Broker	No	No
CVE-2024-38157 Azure IoT SDK	Azure IoT SDK	No	No
CVE-2024-38158 Azure IoT SDK	Azure IoT SDK	No	No
CVE-2024-38159 Windows Network Virtualization	Network Virtualization	No	No

CVE	Component	Public	Exploited
CVE-2024-38160 Windows Network Virtualization	Network Virtualization	No	No
CVE-2024-38161 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-38162 Azure Connected Machine Agent	Azure Connected Machine Agent	No	No
CVE-2024-38163 Windows Update Stack	Update Stack	No	No
CVE-2024-38165 Windows Compressed Folder	Compressed Folder	No	No
CVE-2024-38166 Microsoft Dynamics	Dynamics 365 Cross-site Scripting	No	No
CVE-2024-38167 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-38168 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-38169 Microsoft Office Visio	Office Visio	No	No
CVE-2024-38170 Microsoft Office Excel	Excel	No	No
CVE-2024-38171 Microsoft Office PowerPoint	PowerPoint	No	No
CVE-2024-38172 Microsoft Office Excel	Excel	No	No
CVE-2024-38173 Microsoft Office Outlook	Outlook	No	No
CVE-2024-38177 Windows App Installer	App Installer	No	No
CVE-2024-38178 Windows Scripting	Scripting Engine Memory Corruption Vulnerability	No	Yes
CVE-2024-38180 Windows SmartScreen	SmartScreen	No	No

CVE	Component	Public	Exploited
CVE-2024-38184 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-38185 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-38186 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-38187 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-38189 Microsoft Office Project	Project	No	Yes
CVE-2024-38191 Windows Kernel-Mode Drivers	Kernel Streaming Service Driver	No	No
CVE-2024-38193 Windows Ancillary Function Driver for WinSock	Ancillary Function Driver for WinSock	No	Yes
CVE-2024-38195 Azure CycleCloud	Azure CycleCloud	No	No
CVE-2024-38196 Windows Common Log File System Driver	Common Log File System Driver	No	No
CVE-2024-38197 Microsoft Teams	Teams for iOS	No	No
CVE-2024-38198 Windows Print Spooler Components	Print Spooler	No	No
CVE-2024-38199 Line Printer Daemon Service (LPD)	Line Printer Daemon (LPD) Service	Yes	No
CVE-2024-38200 Microsoft Office	Office	Yes	No
CVE-2024-38201 Azure Stack	Azure Stack Hub	No	No
CVE-2024-38202 Windows Update Stack	Update Stack	Yes	No
CVE-2024-38206 Microsoft Copilot Studio	Copilot Studio	No	No

CVE	Component	Public	Exploited
CVE-2024-38211 Microsoft Dynamics	Dynamics 365 (on-premises) Cross-site Scripting	No	No
CVE-2024-38213 Windows Mark of the Web (MOTW)	Mark of the Web	No	Yes
CVE-2024-38214 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38215 Windows Cloud Files Mini Filter Driver	Cloud Files Mini Filter Driver	No	No
CVE-2024-38218 Microsoft Edge (Chromium-based)	Edge (HTML-based) Memory Corruption	No	No
CVE-2024-38223 Windows Initial Machine Configuration	Initial Machine Configuration	No	No

What is CWE?

- Common Weakness Enumeration
- Community-developed list of common software and hardware weakness types that could have security ramifications
- Enables ‘root cause mapping’ to aid in identifying common patterns to target
- Examples: memory out-of-bounds write, NULL pointer dereference

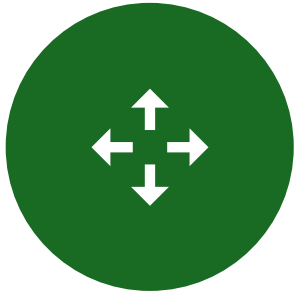
References:

MITRE CWE list: CWE List

MSRC blog on adopting CWE standard

Cloud Service CVEs

Historically ‘no-action’ CVEs in cloud services = no CVE



Starting in June 2024 that changed

Cloud service CVEs that are fixed and require no customer action may still have a CVE published

Toward greater transparency: Unveiling Cloud Service CVEs