Microsoft

Microsoft Security Release

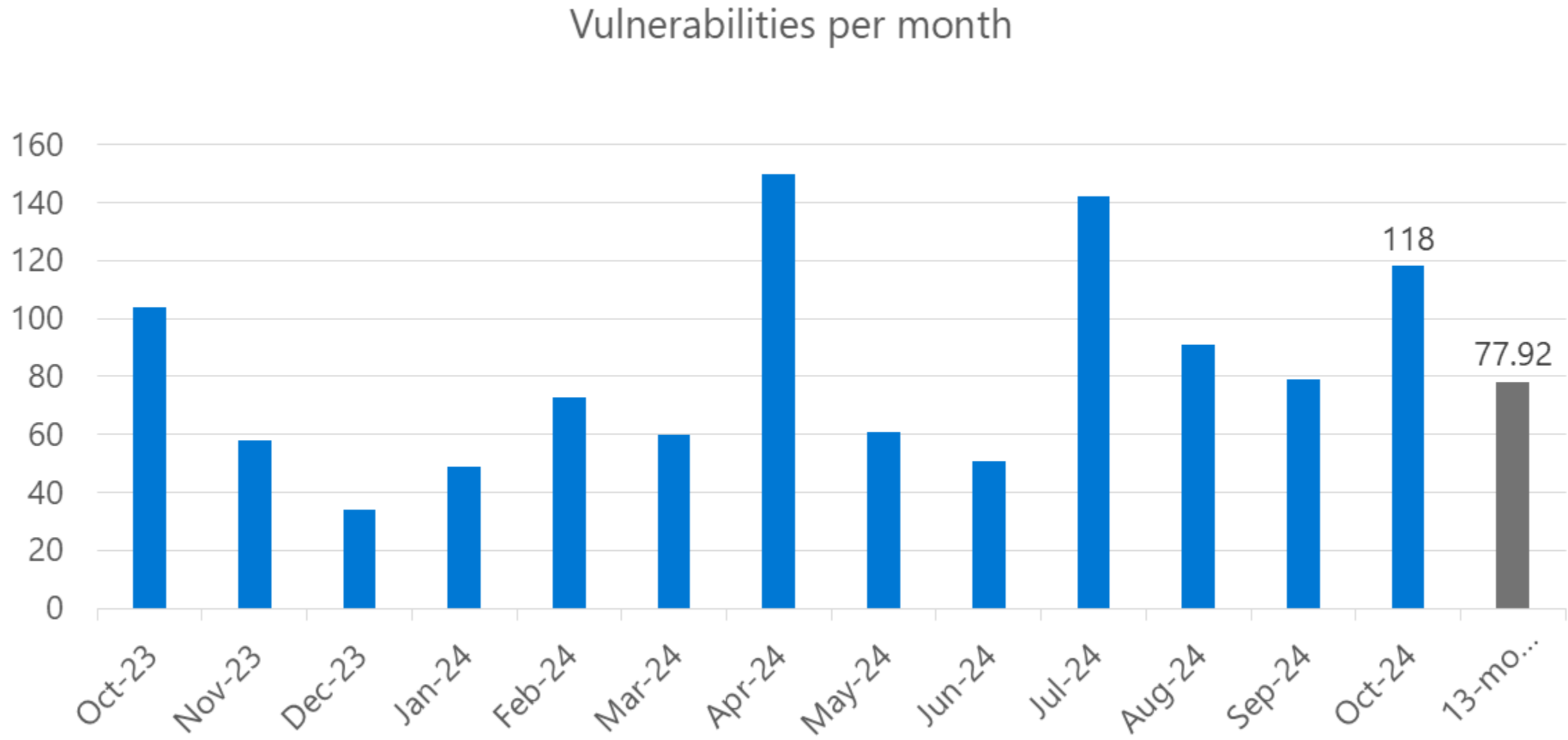
October 8, 2024

Agenda

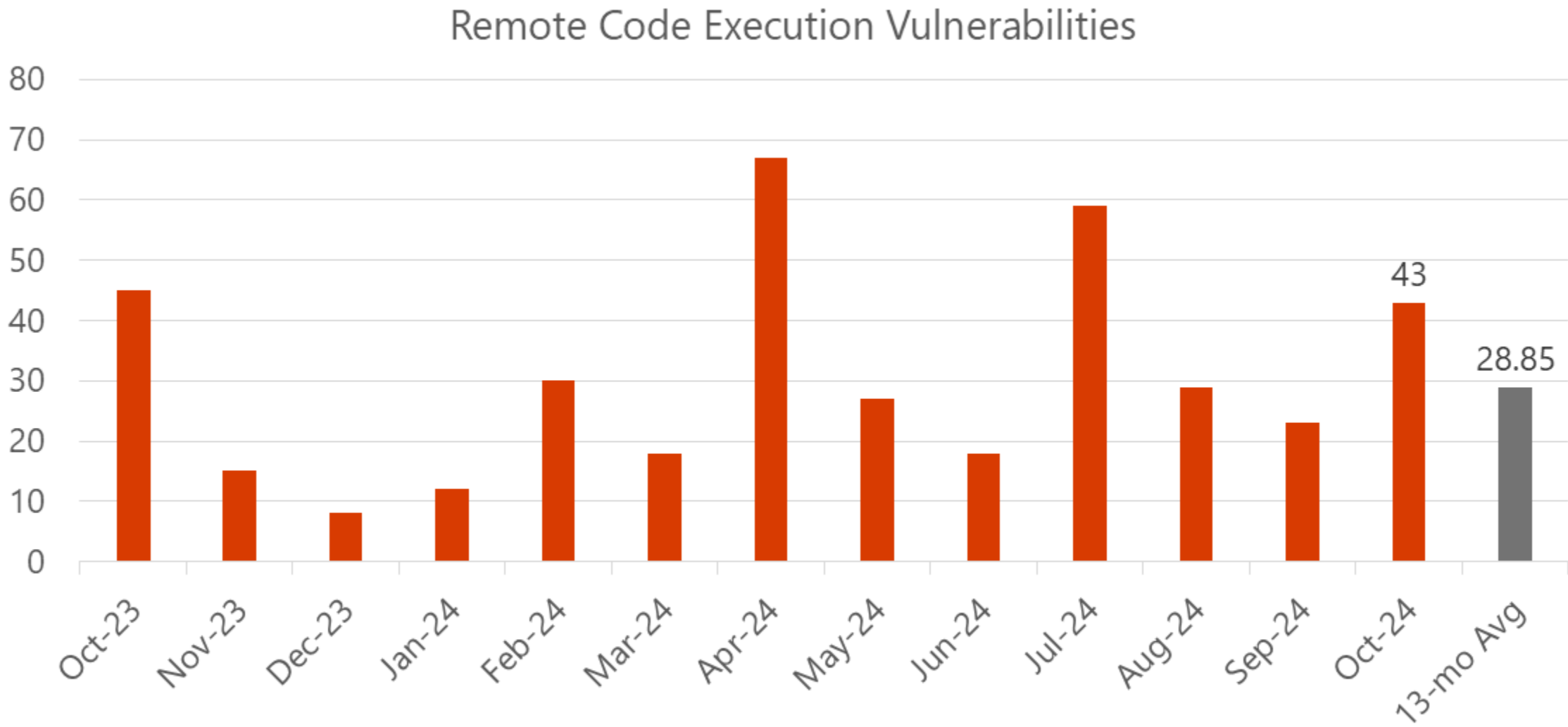
Security Updates

Product Support Lifecyle

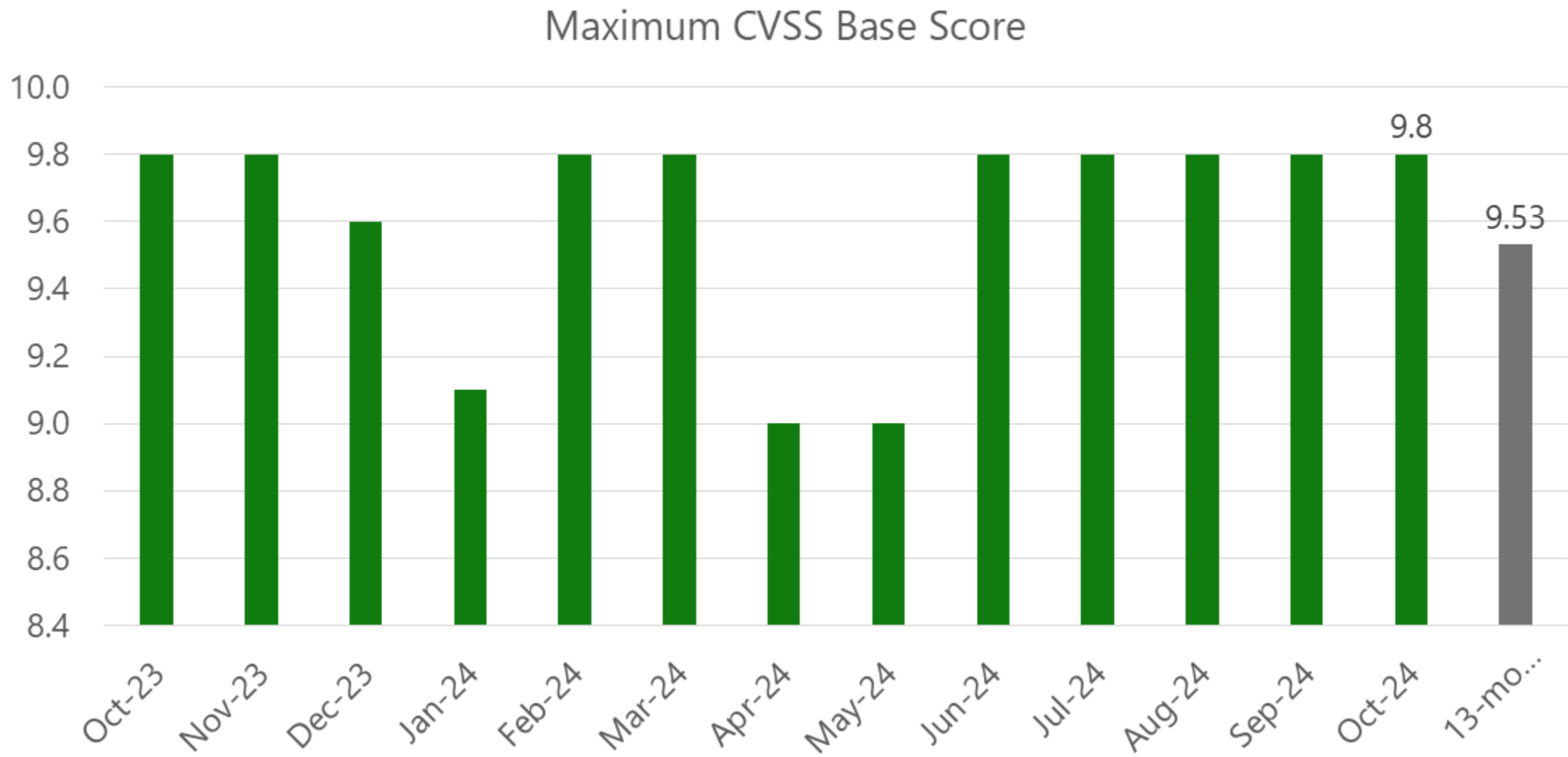
Microsoft


Vulnerabilities per month
160
140
120
100
80
60
40
20
0
118
77.92
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
13-mo...

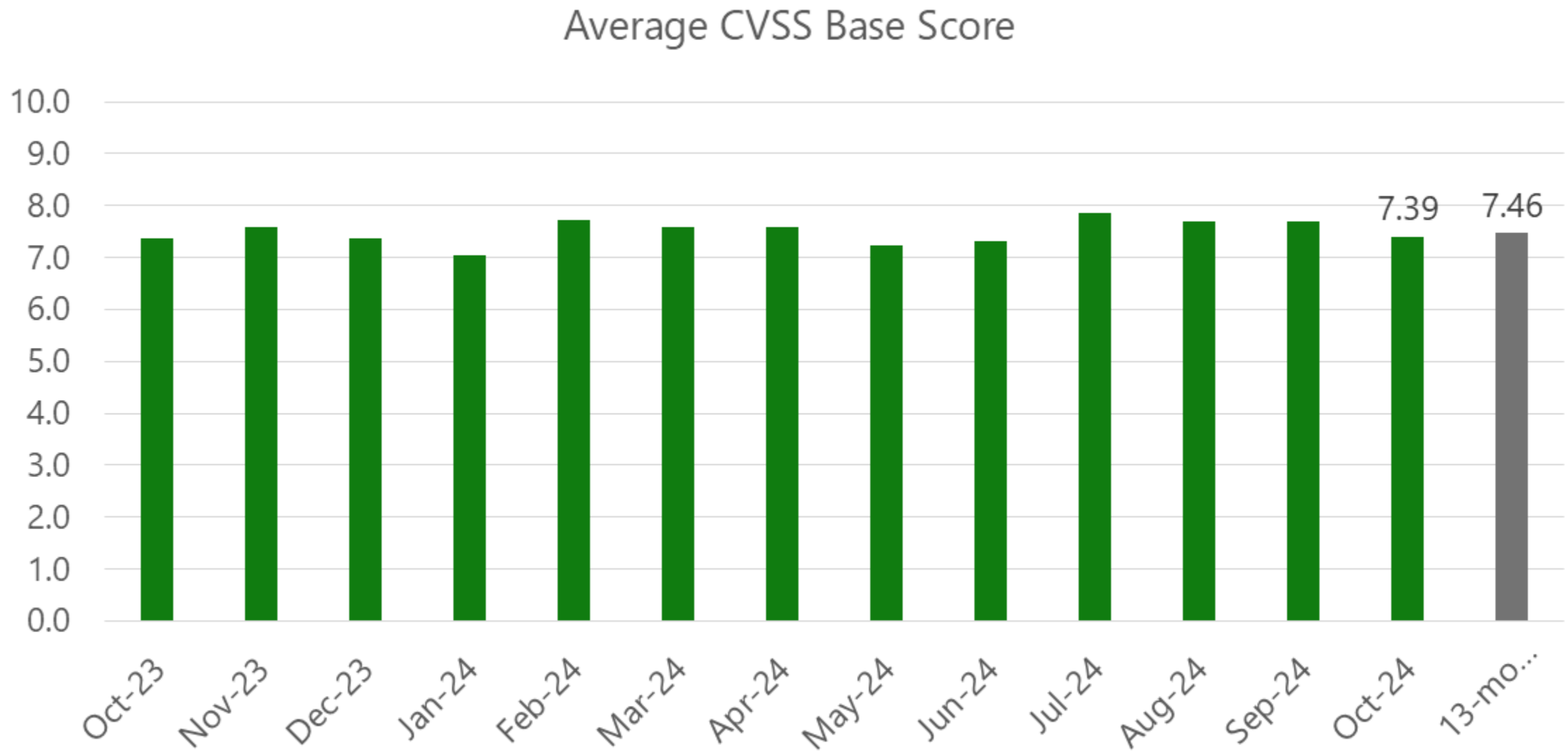
Microsoft


Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
43
28.85
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
13-mo Avg

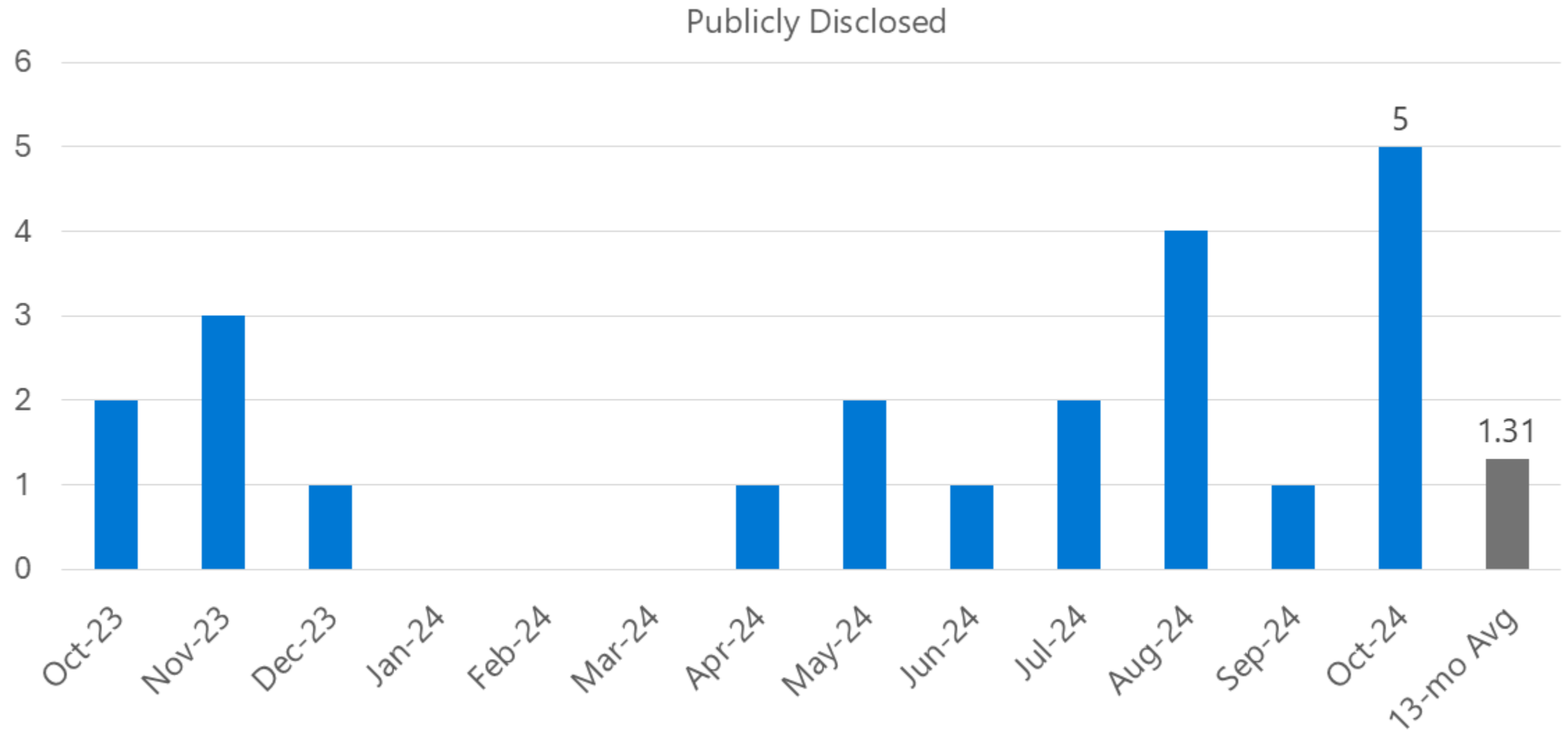
Microsoft


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

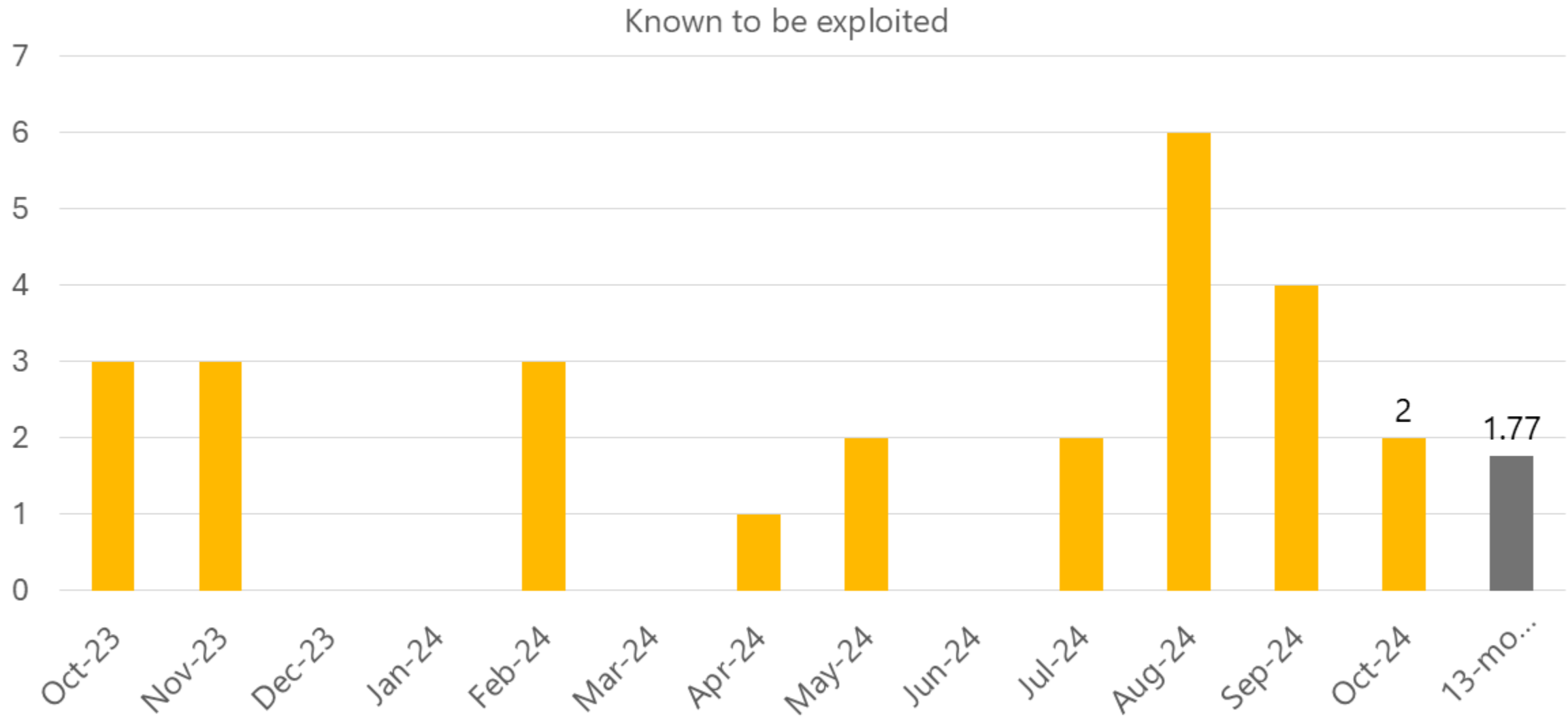
Microsoft


Average CVSS Base Score
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
7.39
7.46
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
13-mo…

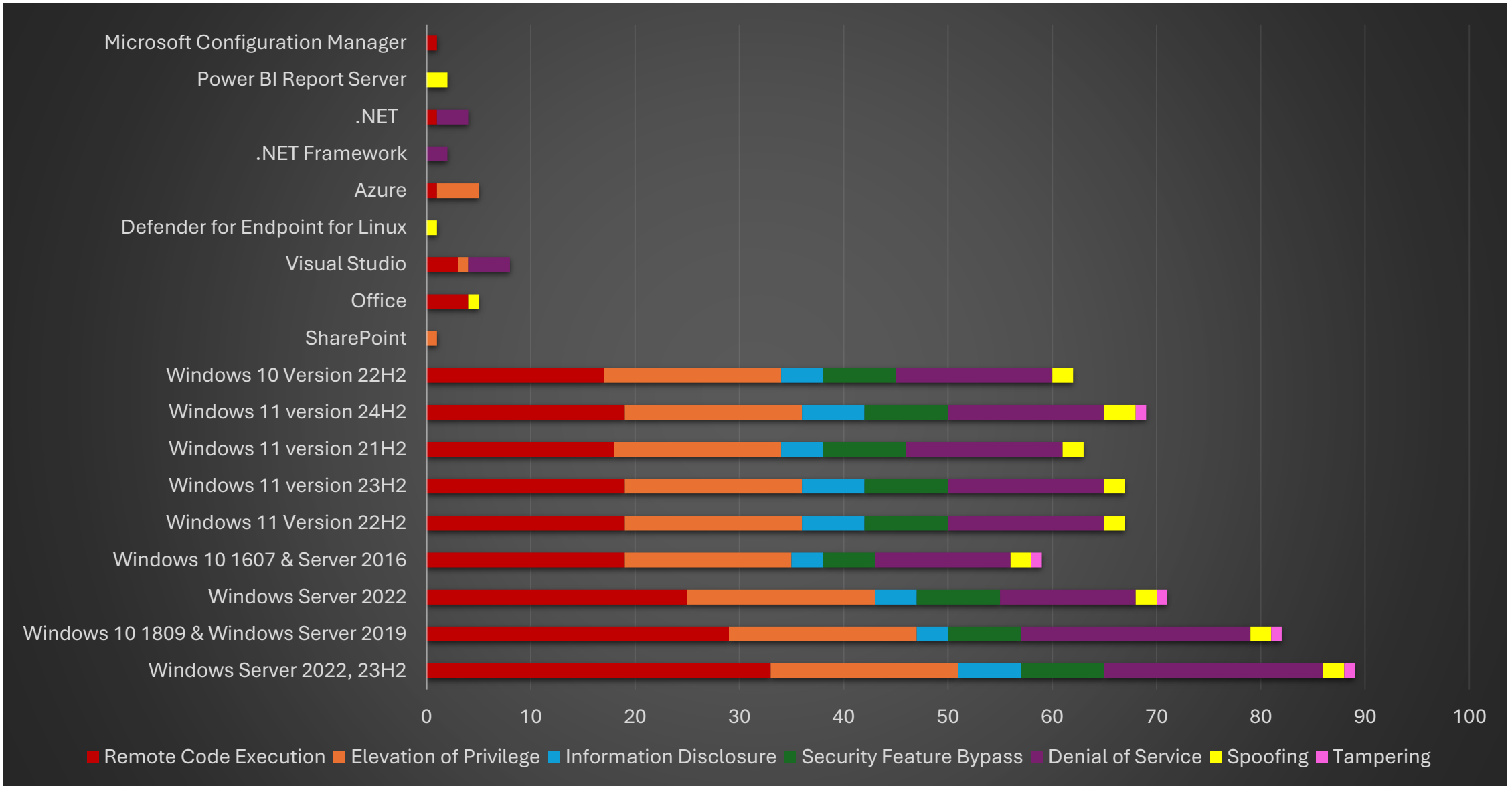
Microsoft


Publicly Disclosed
6
5
4
3
2
1
0
5
1.31
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
13-mo Avg

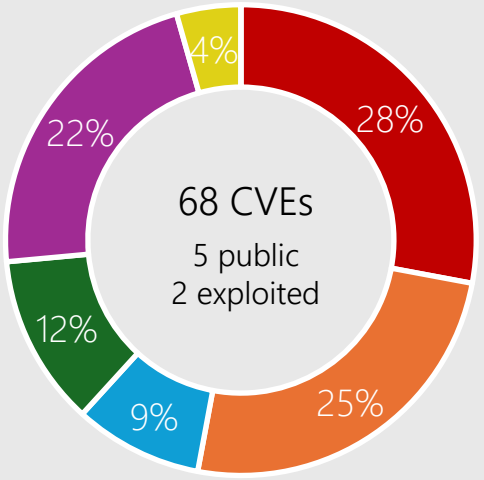
Microsoft


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

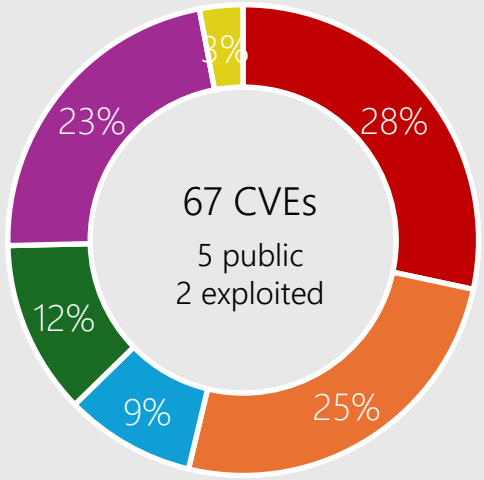
Microsoft Security Release Overview – October 2024



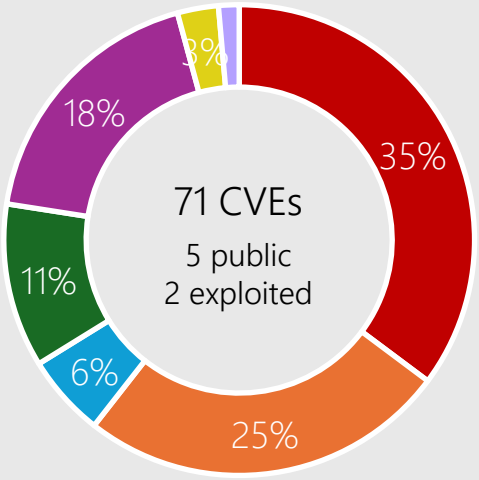
Windows 11, Server 2022



Windows 11 24H2



Windows 11 23H2



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-2024-38124 Netlogon

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.0 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

- Avoid using predictable naming conventions for domain controllers
- Ensure that the secure channel is validated against more than just the computer name of the machine it was delivered to
- Monitor for unexpected computer renaming activities
- Consider enhanced authentication mechanisms

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server 2019
Server 2016

CVE-2024-43582 Remote Desktop Protocol

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

CVE-2024-43572 Microsoft Mgmt Console

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly disclosed | Exploitation detected

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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-20659 Hyper-V

Impact, Severity, Disclosure

Security Feature Bypass | Important | Publicly disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.1 | Attack Vector: Adjacent | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

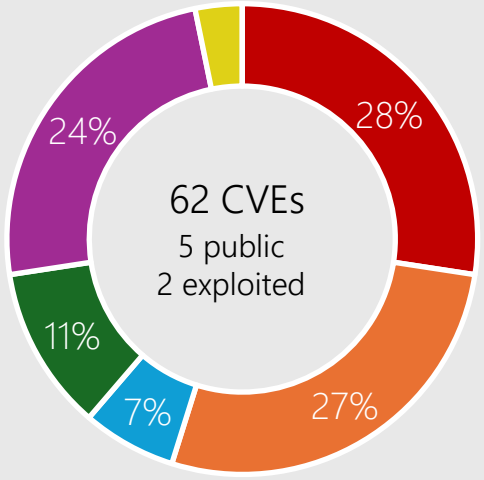
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

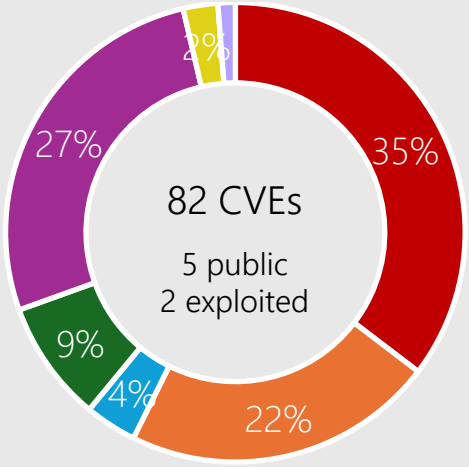
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019

Windows 10



Windows 10 22H2



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-2024-43573 MSHTML Platform

Impact, Severity, Disclosure

Spoofing | Moderate | Publicly disclosed | Exploitation Detected

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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-43583 Winlogon

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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.

More Information

Third party IMEs will be blocked during the logon process. See KB5046254: Vulnerability when using a third-party Input Method Editor at the Microsoft Windows sign in screen.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-6197 Curl

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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.

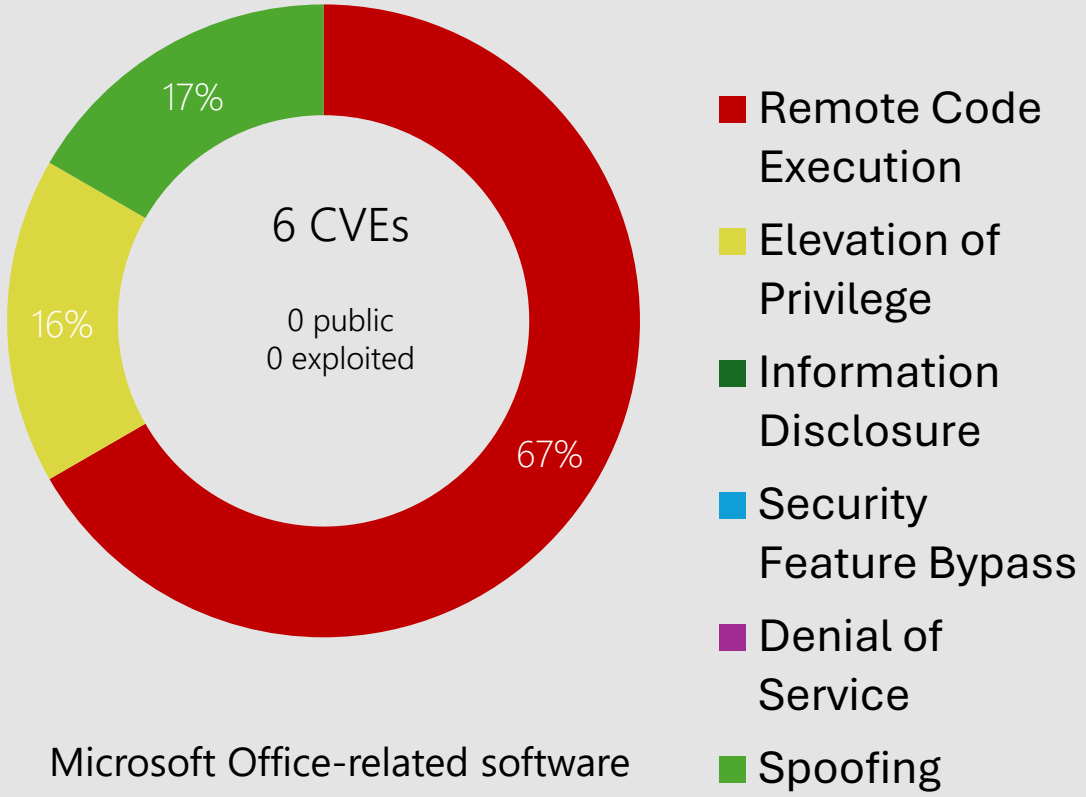
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019

Windows CVEs: CVSS 8.8

- CVE-2024-43519 WDAC OLE DB provider for SQL
- CVE-2024-43532 Remote Registry Service
- CVE-2024-43533 Remote Desktop Client
- CVE-2024-43611 RRAS
- CVE-2024-43517 ActiveX Data Objects

Microsoft Office



Microsoft Office-related software

Products:

Office 2016
Office 2019
Excel 2016
365 Apps Enterprise
Office LTSC 2021
Office LTSC 2024
SharePoint Server Subscription Edition
SharePoint Enterprise Server 2016
SharePoint Server 2019

CVE-2024-43504 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 2019
Excel 2016
Office 365 Apps for Enterprise
Office LTSC 2021/2024

CVE-2024-43503 SharePoint

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

SharePoint Subscription Edition
SharePoint 2019
SharePoint Ent 2016

Other Products

Configuration Manager

CVE-2024-43468 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Microsoft Configuration Manager 2303, Microsoft Configuration Manager 2309, Microsoft Configuration Manager 2403

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-43488 | Visual Studio Code extension for Arduino Remote Code Execution Vulnerability

Base CVSS: 8.8 | **Max Severity**: Critical | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: Required

Affected Products: Visual Studio Code extension for Arduino *Note: this extension has been deprecated. Microsoft recommends using Arduino IDE software

---

CVE-2024-38229 | .NET and Visual Studio Remote Code Execution Vulnerability

Base CVSS: 8.1 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: None | **User Interaction Required**: None

Affected Products: .NET 8.0, Visual Studio 2022

CVE-2024-43601 | Visual Studio Code for Linux Remote Code Execution Vulnerability

Base CVSS: 7.1 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: Low | **User Interaction Required**: Required

Affected Products: Visual Studio Code

Developer Tools

Microsoft .NET, .NET Framework, Visual Studio, Visual C++

CVE-2024-43590 | Visual C++ Redistributable Installer Elevation of Privilege Vulnerability

Base CVSS: 7.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None

Affected Products: Visual Studio 2022, Visual Studio 2019, Visual Studio 2017, Visual C++ Redistributable Installer

---

CVE-2024-43483/43484 | .NET, .NET Framework, and Visual Studio Denial of Service Vulnerability

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 Framework, .NET 6.0, .NET 8.0, Visual Studio 2022

CVE-2024-43485 | .NET, and Visual Studio Denial of Service

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 6.0, .NET 8.0, Visual Studio 2022

Developer Tools

Visual Studio

CVE-2024-43603 | Visual Studio Collector Service Denial of Service Vulnerability

Base CVSS: 5.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None

Affected Products: Visual Studio 2022, Visual Studio 2019, Visual Studio 2017, Visual Studio 2015

Other Products

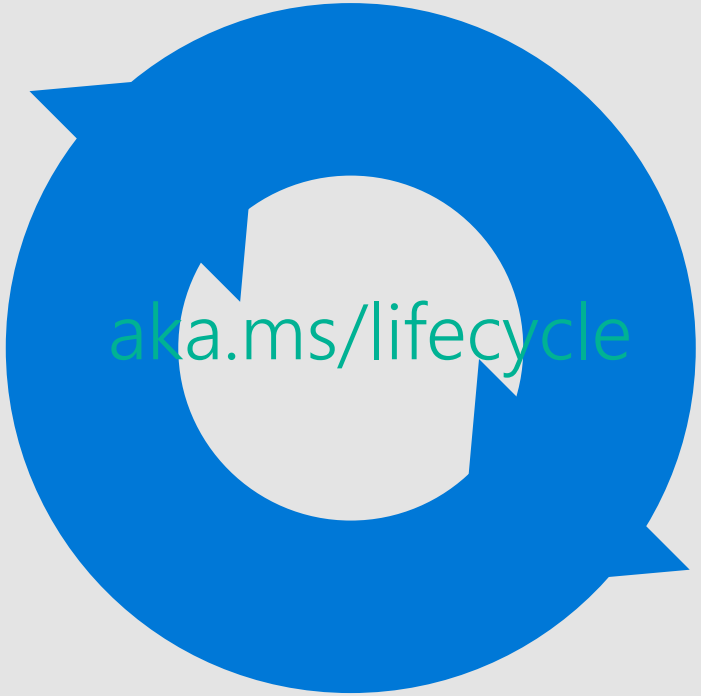
Azure, Apps, Defender for Linux

CVE-2024-38179 Azure Stack
CVE-2024-43591 Azure CLI
CVE-2024-43497 DeepSpeed
CVE-2024-43614 Microsoft Defender for Endpoint for Linux
CVE-2024-43481/43612 Power BI Report Server
CVE-2024-38097 Azure Monitor Agent
CVE-2024-43480 Azure Service Fabric for Linux
CVE-2024-43604 Outlook for Android
CVE-2024-43533 Remote Desktop Client for Windows Desktop

Product Lifecycle Update

Products reaching end of servicing in October

Windows 11 21H2 Ent & EDU
Windows 11 22H2 Home & Pro
Configuration Mgr version 2303
Dynamics 365 Business Central on-premises (Modern Policy), 2023 release wave 1, version 22.x



Microsoft

Questions?

Appendix

CVE	Component	Public	Exploited
CVE-2024-20659 Role: Windows Hyper-V	Hyper-V	Yes	No
CVE-2024-30092 Windows Hyper-V	Hyper-V	No	No
CVE-2024-37976 Windows EFI Partition	Resume Extensible Firmware Interface	No	No
CVE-2024-37979 Windows Kernel	Kernel	No	No
CVE-2024-37982 Windows EFI Partition	Resume Extensible Firmware Interface	No	No
CVE-2024-37983 Windows EFI Partition	Resume Extensible Firmware Interface	No	No
CVE-2024-38029 OpenSSH for Windows	OpenSSH for Windows	No	No
CVE-2024-38097 Azure Monitor	Azure Monitor Agent	No	No
CVE-2024-38124 Windows Netlogon	Netlogon	No	No
CVE-2024-38129 Windows Kerberos	Kerberos	No	No
CVE-2024-38149 BranchCache	BranchCache	No	No
CVE-2024-38179 Azure Stack	Azure Stack Hyperconverged Infrastructure (HCI)	No	No
CVE-2024-38212 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38229 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-38261 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-38262 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-38265 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No

CVE	Component	Public	Exploited
CVE-2024-43453 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43456 Windows Remote Desktop Services	Remote Desktop Services	No	No
CVE-2024-43468 Microsoft Configuration Manager	Configuration Manager	No	No
CVE-2024-43480 Service Fabric	Azure Service Fabric for Linux	No	No
CVE-2024-43481 Power BI	Power BI Report Server	No	No
CVE-2024-43483 .NET, .NET Framework, Visual Studio	.NET, .NET Framework, and Visual Studio	No	No
CVE-2024-43484 .NET, .NET Framework, Visual Studio	.NET, .NET Framework, and Visual Studio	No	No
CVE-2024-43485 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-43488 Visual Studio Code	Visual Studio Code extension for Arduino	No	No
CVE-2024-43497 DeepSpeed	DeepSpeed	No	No
CVE-2024-43500 Windows Resilient File System (ReFS)	Resilient File System (ReFS)	No	No
CVE-2024-43501 Windows Common Log File System Driver	Common Log File System Driver	No	No
CVE-2024-43502 Windows Kernel	Kernel	No	No
CVE-2024-43503 Microsoft Office SharePoint	SharePoint	No	No
CVE-2024-43504 Microsoft Office Excel	Excel	No	No
CVE-2024-43505 Microsoft Office Visio	Office Visio	No	No
CVE-2024-43506 BranchCache	BranchCache	No	No

CVE	Component	Public	Exploited
CVE-2024-43508 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-43509 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-43511 Windows Kernel	Kernel	No	No
CVE-2024-43512 Windows Standards-Based Storage Management Service	Standards-Based Storage Management Service	No	No
CVE-2024-43513 Windows BitLocker	BitLocker	No	No
CVE-2024-43514 Windows NTFS	Resilient File System (ReFS)	No	No
CVE-2024-43515 Internet Small Computer Systems Interface (iSCSI)	Internet Small Computer Systems Interface (iSCSI)	No	No
CVE-2024-43516 Windows Secure Kernel Mode	Secure Kernel Mode	No	No
CVE-2024-43517 Microsoft ActiveX	ActiveX Data Objects	No	No
CVE-2024-43518 Windows Telephony Server	Telephony Server	No	No
CVE-2024-43519 Microsoft WDAC OLE DB provider for SQL	WDAC OLE DB provider for SQL Server	No	No
CVE-2024-43520 Windows Kernel	Kernel	No	No
CVE-2024-43521 Role: Windows Hyper-V	Hyper-V	No	No
CVE-2024-43522 Windows Local Security Authority (LSA)	Local Security Authority (LSA)	No	No
CVE-2024-43523 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43524 Windows Mobile Broadband	Mobile Broadband Driver	No	No

CVE	Component	Public	Exploited
CVE-2024-43526 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43527 Windows Kernel	Kernel	No	No
CVE-2024-43528 Windows Secure Kernel Mode	Secure Kernel Mode	No	No
CVE-2024-43529 Windows Print Spooler Components	Print Spooler	No	No
CVE-2024-43532 RPC Endpoint Mapper Service	Remote Registry Service	No	No
CVE-2024-43533 Remote Desktop Client	Remote Desktop Client	No	No
CVE-2024-43534 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-43535 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-43536 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43537 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43538 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43540 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43541 Microsoft Simple Certificate Enrollment Protocol	Simple Certificate Enrollment Protocol	No	No
CVE-2024-43542 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43543 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43544 Microsoft Simple Certificate Enrollment Protocol	Simple Certificate Enrollment Protocol	No	No

CVE	Component	Public	Exploited
CVE-2024-43545 Windows Online Certificate Status Protocol (OCSP)	Online Certificate Status Protocol (OCSP) Server	No	No
CVE-2024-43546 Windows Cryptographic Services	Cryptographic	No	No
CVE-2024-43547 Windows Kerberos	Kerberos	No	No
CVE-2024-43549 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43550 Windows Secure Channel	Secure Channel	No	No
CVE-2024-43551 Windows Storage	Storage	No	No
CVE-2024-43552 Windows Shell	Shell	No	No
CVE-2024-43553 Windows NT OS Kernel	NT OS Kernel	No	No
CVE-2024-43554 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-43555 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43556 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-43557 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43558 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43559 Windows Mobile Broadband	Mobile Broadband Driver	No	No
CVE-2024-43560 Windows Storage Port Driver	Windows Storage Port Driver	No	No
CVE-2024-43561 Windows Mobile Broadband	Mobile Broadband Driver	No	No

CVE	Component	Public	Exploited
CVE-2024-43562 Windows Network Address Translation (NAT)	Network Address Translation (NAT)	No	No
CVE-2024-43563 Windows Ancillary Function Driver for WinSock	Ancillary Function Driver for WinSock	No	No
CVE-2024-43564 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43565 Windows Network Address Translation (NAT)	Network Address Translation (NAT)	No	No
CVE-2024-43567 Role: Windows Hyper-V	Hyper-V	No	No
CVE-2024-43570 Windows Kernel	Kernel	No	No
CVE-2024-43571 Sudo for Windows	Sudo for Windows	No	No
CVE-2024-43572 Microsoft Management Console	Management Console	Yes	Yes
CVE-2024-43573 Windows MSHTML Platform	MSHTML Platform	Yes	Yes
CVE-2024-43574 Microsoft Windows Speech	Speech Application Programming Interface (SAPI)	No	No
CVE-2024-43575 Role: Windows Hyper-V	Hyper-V	No	No
CVE-2024-43576 Microsoft Office	Office	No	No
CVE-2024-43581 OpenSSH for Windows	OpenSSH for Windows	No	No
CVE-2024-43582 Windows Remote Desktop	Remote Desktop Protocol Server	No	No
CVE-2024-43583 Winlogon	Winlogon	Yes	No
CVE-2024-43584 Windows Scripting	Scripting Engine	No	No

CVE	Component	Public	Exploited
CVE-2024-43585 Code Integrity Guard	Code Integrity Guard	No	No
CVE-2024-43589 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43590 Visual C++ Redistributable Installer	Visual C++ Redistributable Installer	No	No
CVE-2024-43591 Azure CLI	Azure Command Line Integration (CLI)	No	No
CVE-2024-43592 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43593 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43599 Remote Desktop Client	Remote Desktop Client	No	No
CVE-2024-43601 Visual Studio Code	Visual Studio Code for Linux	No	No
CVE-2024-43603 Visual Studio	Visual Studio Collector Service	No	No
CVE-2024-43604 Outlook for Android	Outlook for Android	No	No
CVE-2024-43607 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43608 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43609 Microsoft Office	Office	No	No
CVE-2024-43611 Windows Routing and Remote Access Service (RRAS)	Routing and Remote Access Service (RRAS)	No	No
CVE-2024-43612 Power BI	Power BI Report Server	No	No
CVE-2024-43614 Microsoft Defender for Endpoint	Defender for Endpoint for Linux	No	No

CVE	Component	Public	Exploited
CVE-2024-43615 OpenSSH for Windows	OpenSSH for Windows	No	No
CVE-2024-43616 Microsoft Office	Office	No	No
CVE-2024-6197 Windows cURL Implementation	Open Source Curl Remote Code Execution Vulnerability	Yes	No