Microsoft

Microsoft Security Release

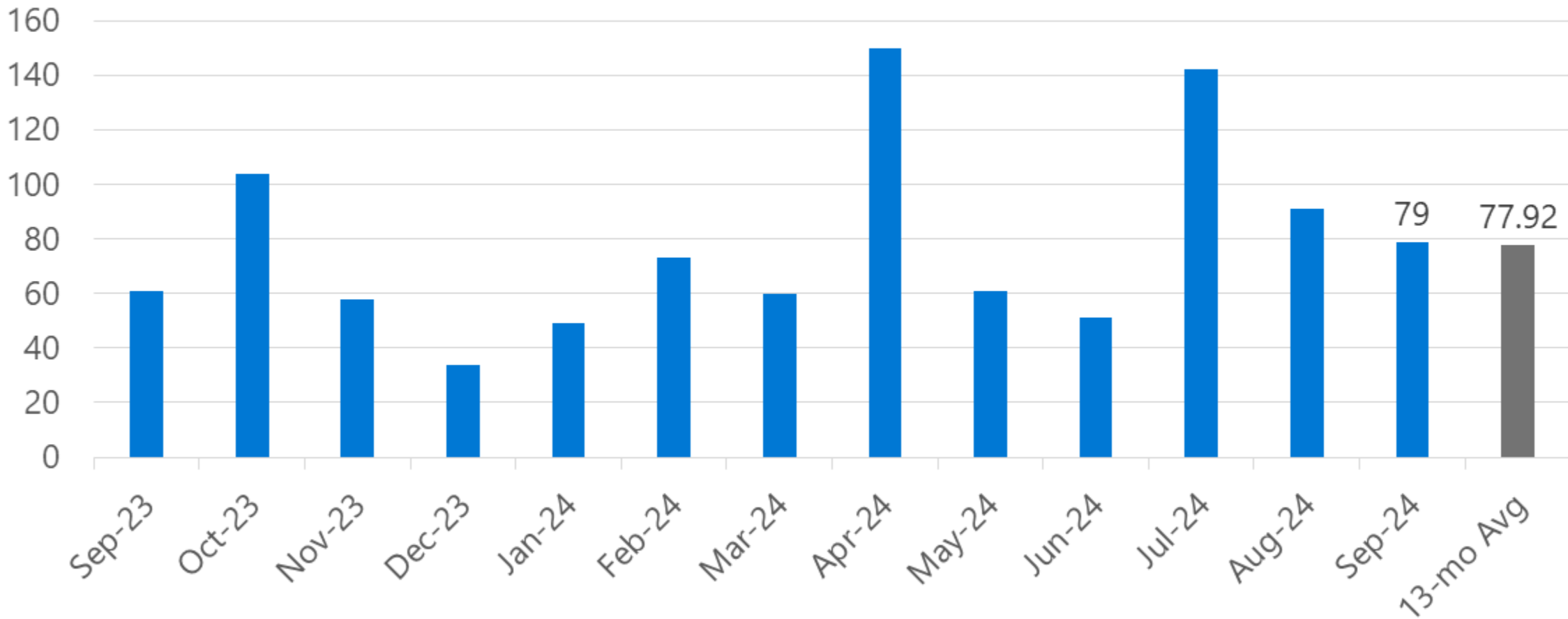
September 10, 2024

Agenda

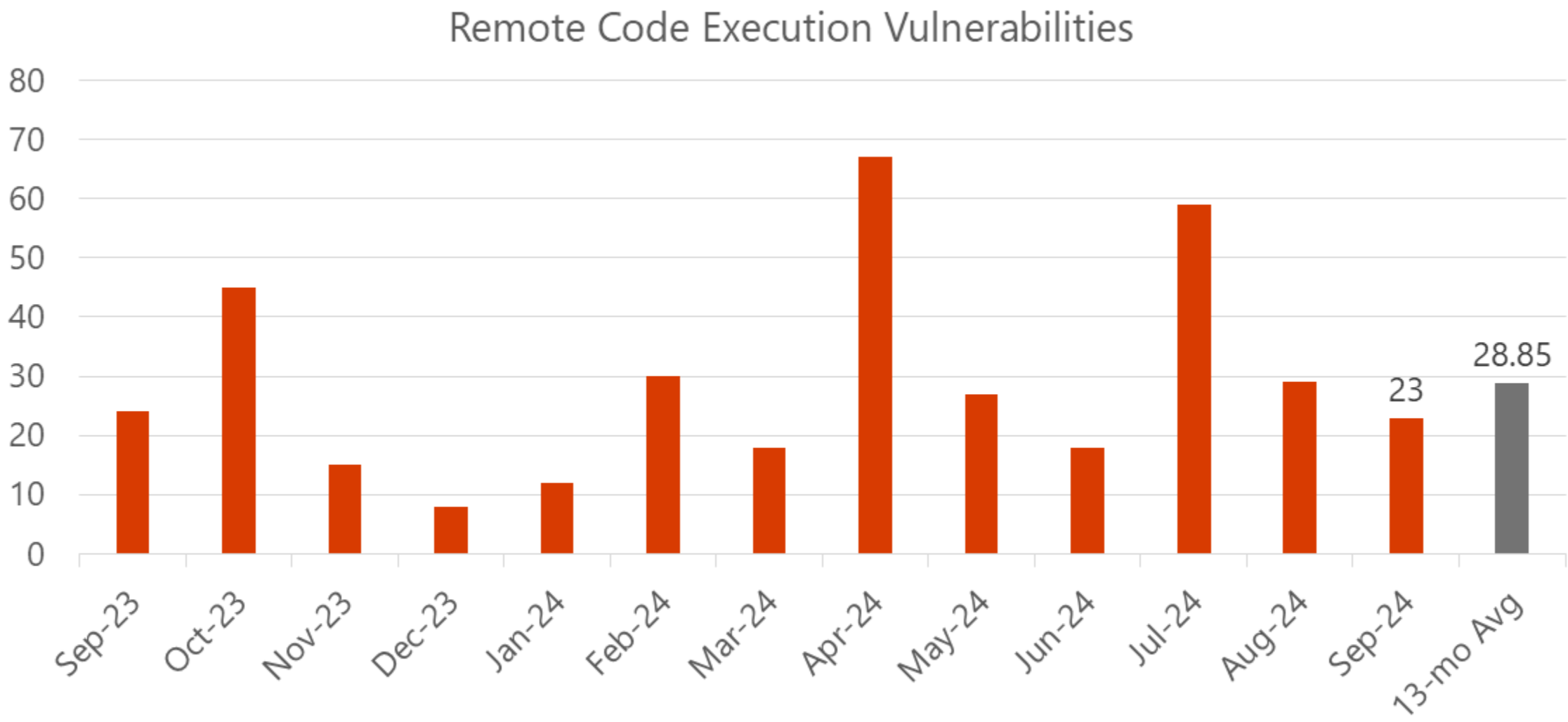
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

Microsoft

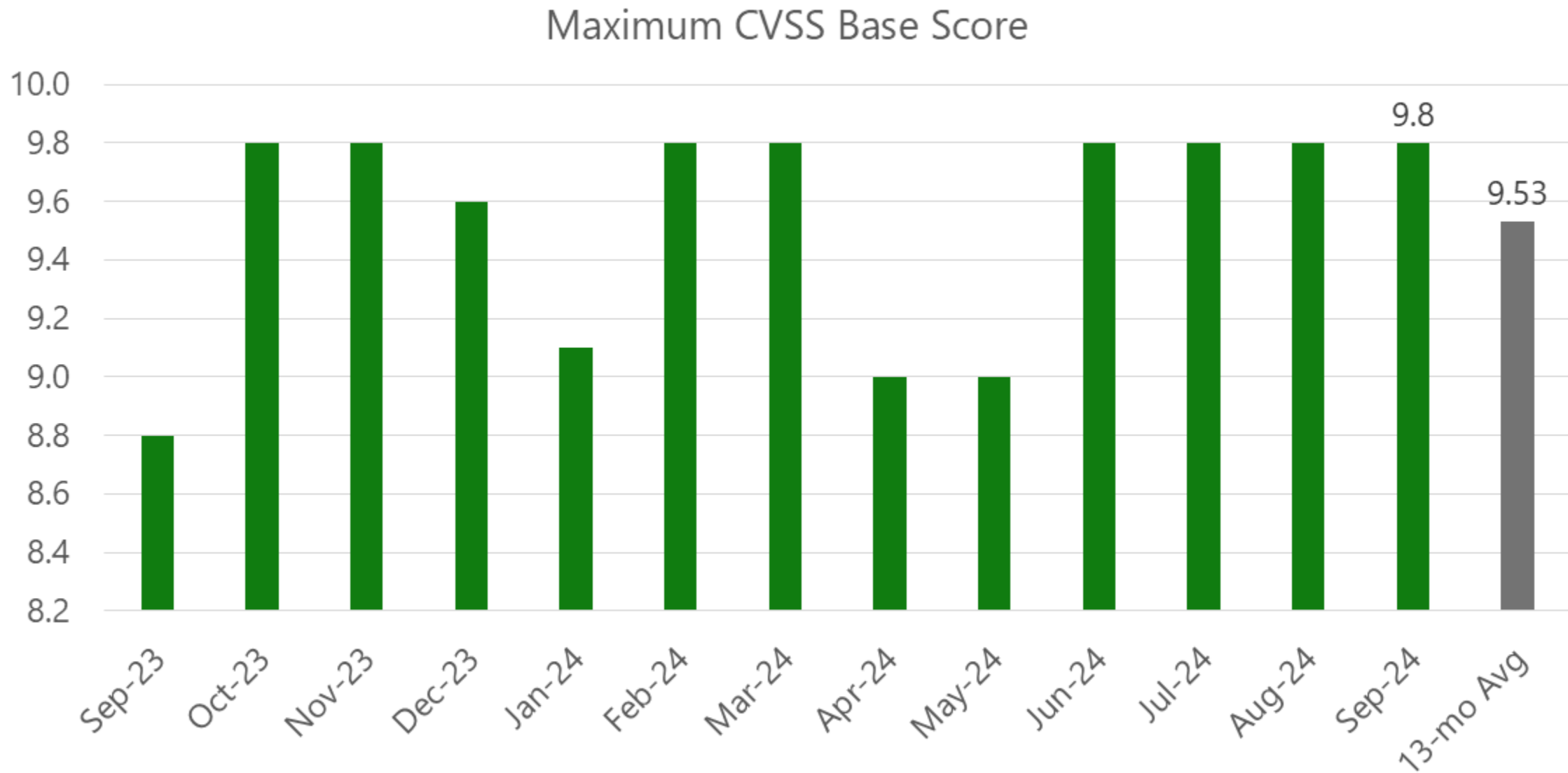
Vulnerabilities per month



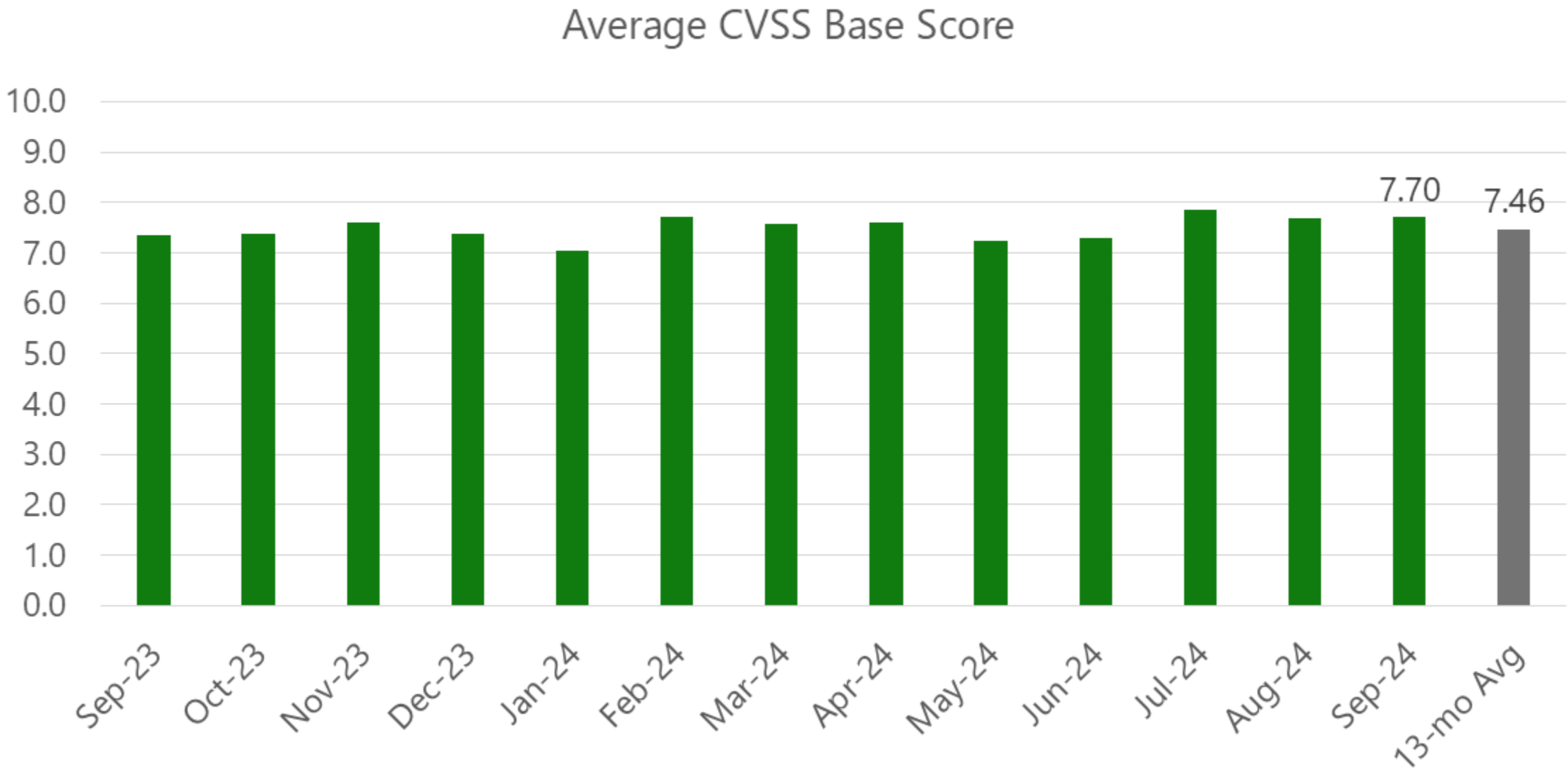
Microsoft


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

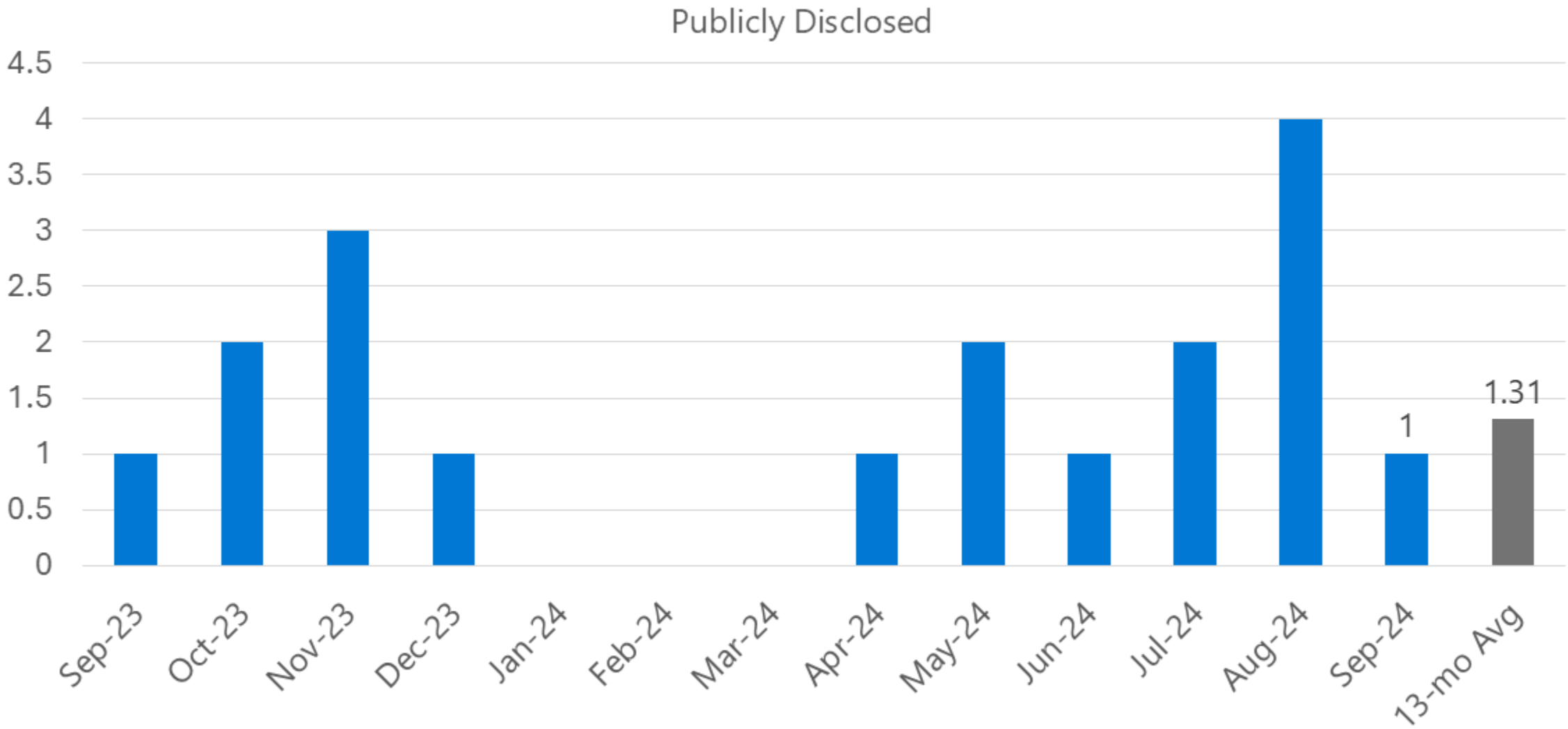
Microsoft


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
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
13-mo Avg

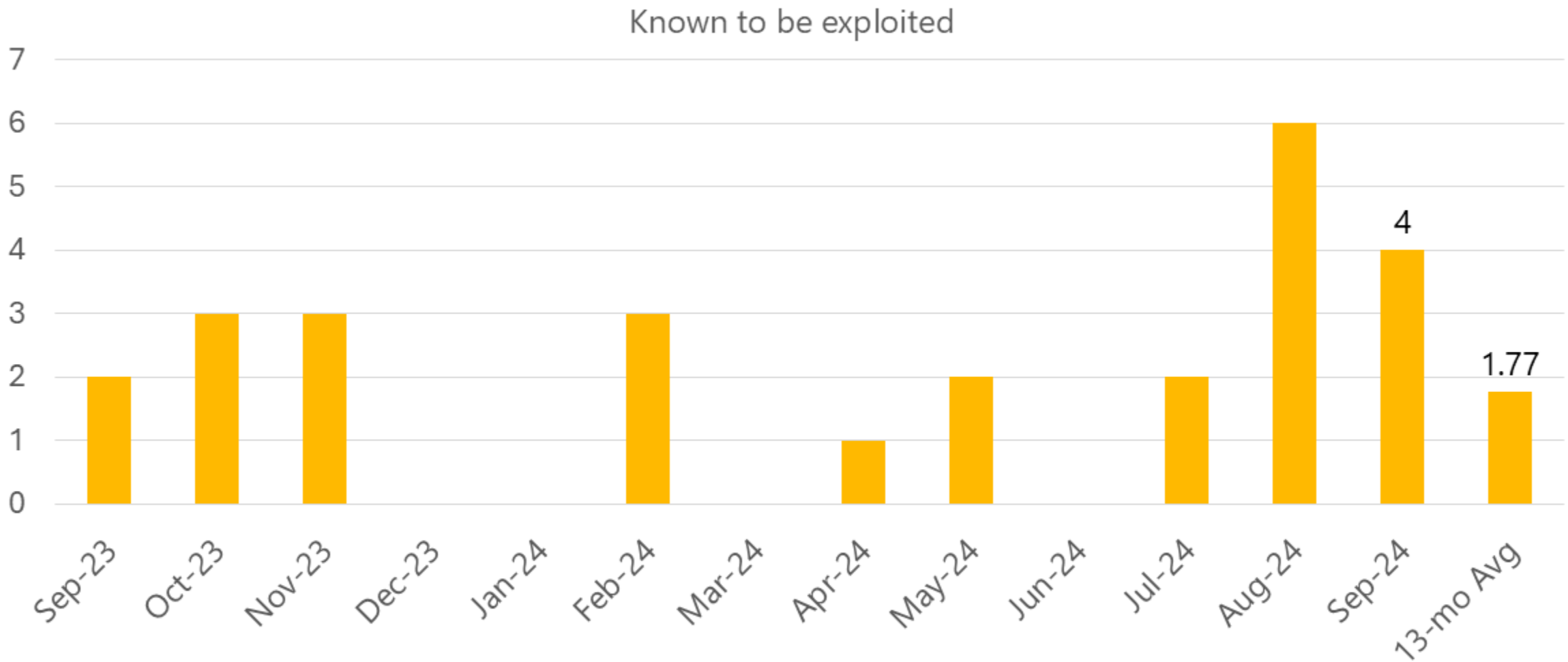
Microsoft


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
7.70
7.46
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
13-mo Avg

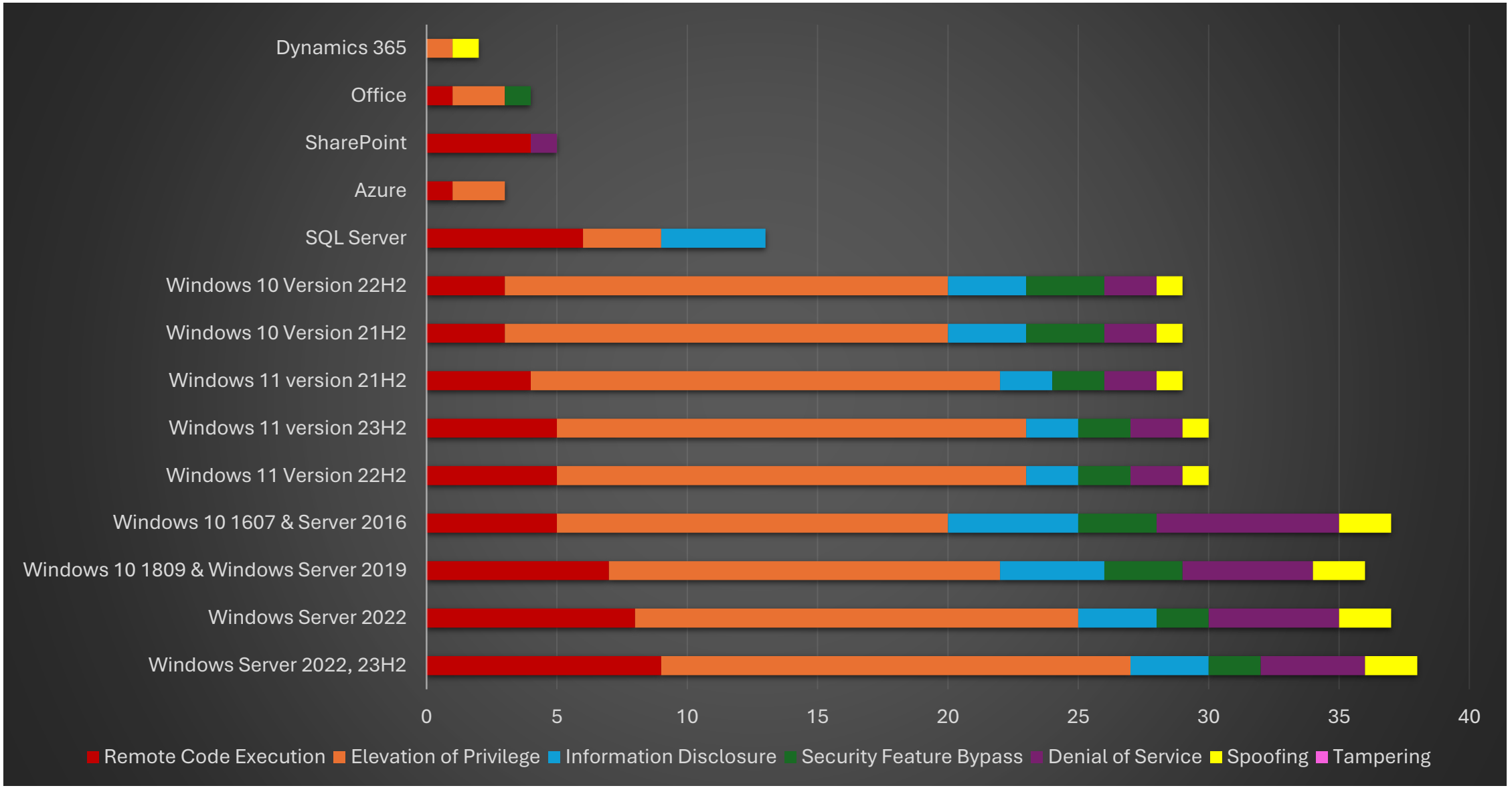
Microsoft


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

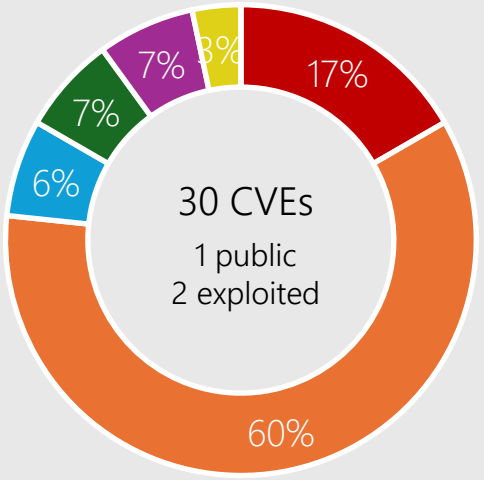
Microsoft


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

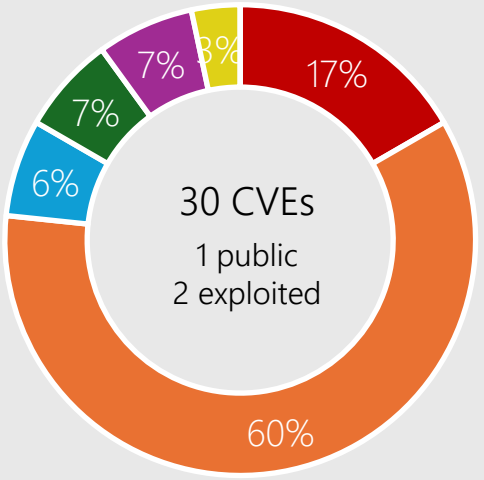
Microsoft Security Release Overview – September 2024



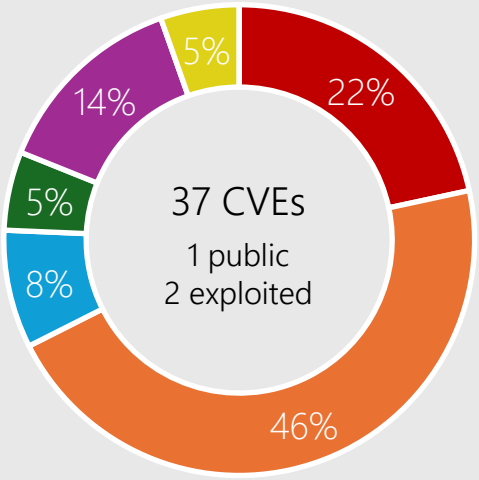
Windows 11, Server 2022



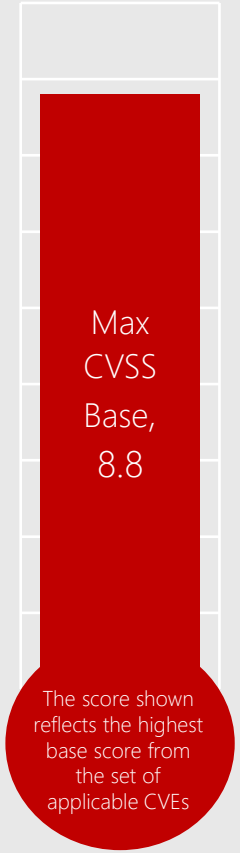
Windows 11 23H2



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-2024-38259 Microsoft Mgmt Console

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
Server 2022

CVE-2024-38014 Windows Installer

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-2024-38260 RD Licensing Service

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: 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

Server 2022
Server 2019
Server 2016

CVE-2024-38119 Network Address Translation

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

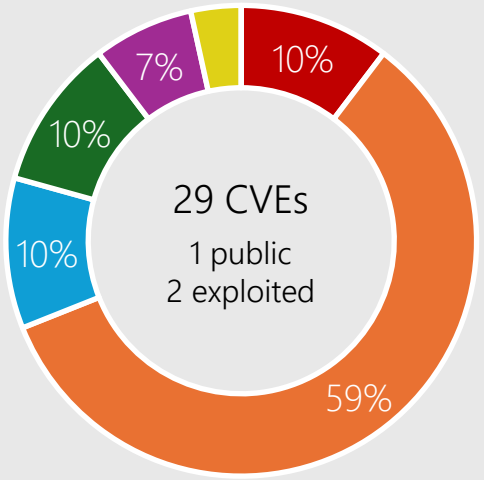
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

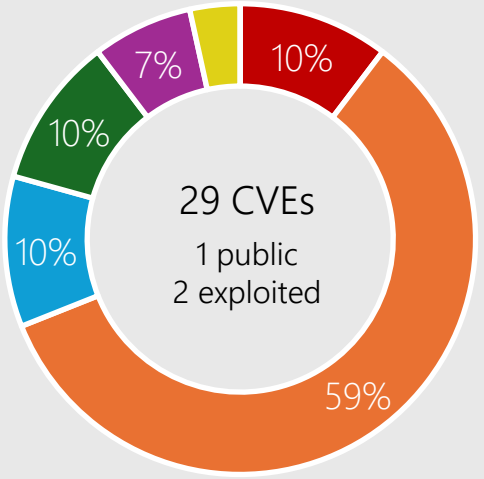
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

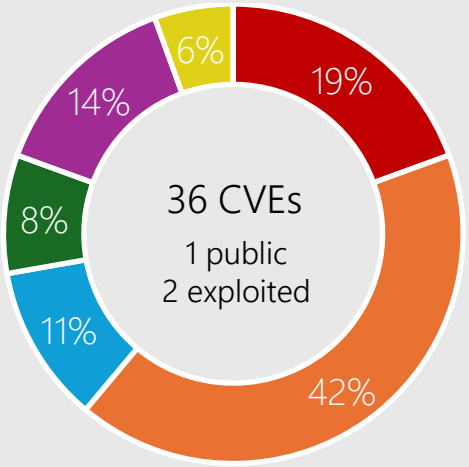
Windows 10



Windows 10 22H2

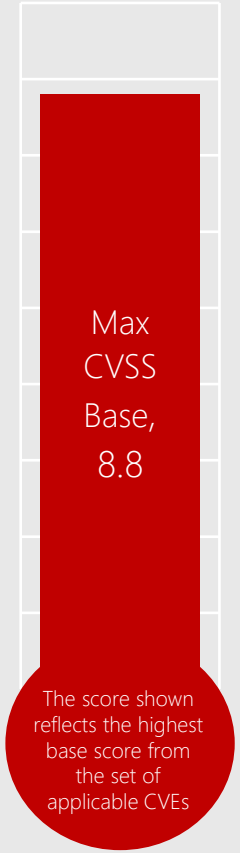


Windows 10 21H2



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-2024-38217 MOTW

Impact, Severity, Disclosure

Security Feature Bypass | Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 5.4 | 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-2024-21416 TCP/IP

Impact, Severity, Disclosure

Remote Code Execution | Important | 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-2024-38240 Remote Access Conn Mgr

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: 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

CVE-2024-43491 Windows Update

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 9.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

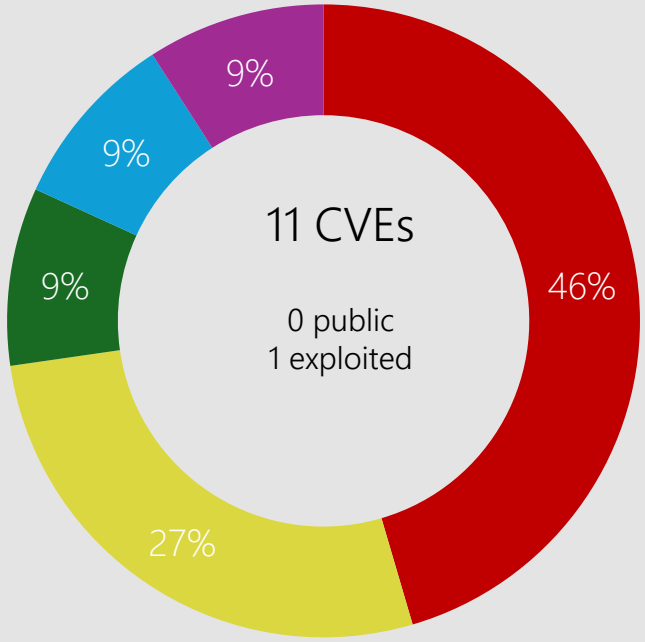
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 10 v.1507 LTSB

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
Publisher 2016
Excel 2016
Visio 2016
365 Apps Enterprise
Office LTSC 2021
Office LTSC for Mac 2021
SharePoint Server Subscription Edition
SharePoint Enterprise Server 2016
SharePoint Server 2019
Office Online Server

CVE-2024-38226 Publisher

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately Disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 7.3 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | 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

Publisher 2016
Office 2016
Office 2019
Office LTSC 2021

CVE-2024-43465 Excel

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: 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 2016
Office 2019
Office 365 Apps for Enterprise
Office LTSC 2021
Office Online Server

CVE-2024-38018 SharePoint

Impact, Severity, Disclosure

Remote Code Execution | Critical | 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 Subscription Edition
SharePoint 2019
SharePoint Ent 2016

SQL Server & Drivers

6 CVEs | SQL Server Native Scoring Remote Code Execution Vulnerability

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

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: SQL Server 2022, SQL Server 2019, SQL Server 2017

---

3 CVEs | SQL Server Native Scoring Information Disclosure Vulnerability

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

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: SQL Server 2022, SQL Server 2019, SQL Server 2017

---

3 CVEs | SQL Server Elevation of Privilege Vulnerability

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

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: SQL Server 2022, SQL Server 2017, SQL Server 2016

SQL Server

CVE-2024-43474 | SQL Server Information Disclosure Vulnerability

Base CVSS: 7.6 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: SQL Server 2019, SQL Server 2017

Other Products

Dynamics 365

CVE-2024-38225 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Microsoft Dynamics 365 Business Central 2024 Release Wave 1, Microsoft Dynamics 365 Business Central 2023 Release Wave 1, Microsoft Dynamics 365 Business Central 2023 Release Wave 2

CVE-2024-43476 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Microsoft Dynamics 365 (on-premises) version 9.1

Other Products

Azure, Apps

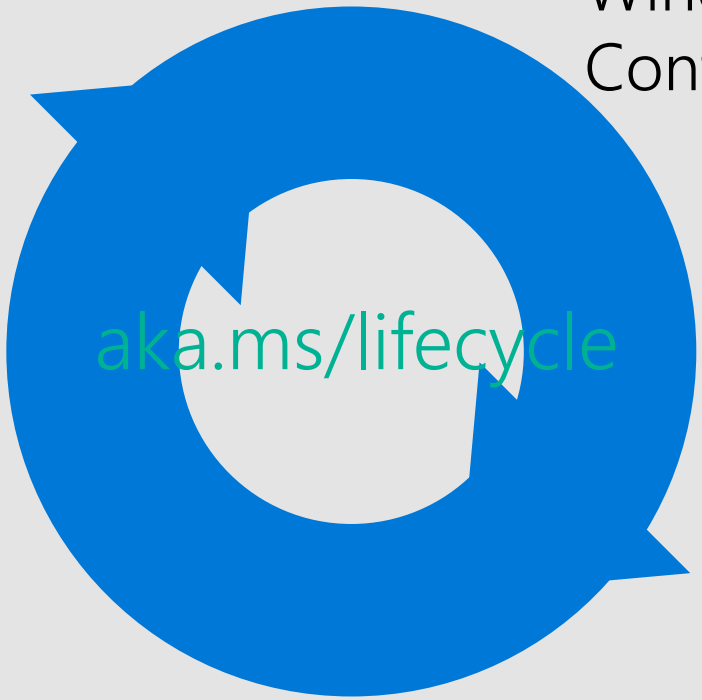
CVE-2024-38188/43470 Azure Network Watcher
CVE-2024-38216/38220 Azure Stack Hub
CVE-2024-43469 Azure Cycle Cloud
CVE-2024-43482 Microsoft Outlook for iOS
CVE-2024-43479 Power Automate

Product Lifecycle Update

Nothing reaching end of support in September

End of Servicing in October

Windows 11 21H2 Ent & EDU
Windows 11 22H2 Home & Pro
Configuration Mgr version 2303



Microsoft

Questions?

Appendix

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

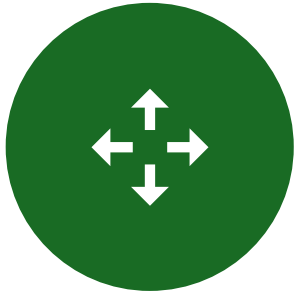
References:

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

CVE	Component	Public	Exploited
CVE-2024-38246 Windows Win32K - GRFX	Win32k	No	No
CVE-2024-38046 Windows PowerShell	PowerShell	No	No
CVE-2024-38237 Microsoft Streaming Service	Kernel Streaming WOW Thunk Service Driver	No	No
CVE-2024-38238 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38241 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38242 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38243 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38244 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38245 Microsoft Streaming Service	Kernel Streaming Service Driver	No	No
CVE-2024-38236 Windows DHCP Server	DHCP Server Service	No	No
CVE-2024-38194 Azure Web Apps	Azure Web Apps	No	No
CVE-2024-38216 Azure Stack	Azure Stack Hub	No	No
CVE-2024-38220 Azure Stack	Azure Stack Hub	No	No
CVE-2024-43470 Azure Network Watcher	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	No	No
CVE-2024-38188 Azure Network Watcher	Azure Network Watcher VM Agent	No	No
CVE-2024-43469 Azure CycleCloud	Azure CycleCloud	No	No
CVE-2024-43491 Windows Update	Windows Update	No	Yes

CVE	Component	Public	Exploited
CVE-2024-43475 Windows Admin Center	Windows Admin Center	No	No
CVE-2024-38252 Windows Win32K - ICOMP	Win32 Kernel Subsystem	No	No
CVE-2024-38253 Windows Win32K - ICOMP	Win32 Kernel Subsystem	No	No
CVE-2024-21416 Windows TCP/IP	TCP/IP	No	No
CVE-2024-38045 Windows TCP/IP	TCP/IP	No	No
CVE-2024-38248 Windows Storage	Storage	No	No
CVE-2024-38230 Windows Standards-Based Storage Management Service	Standards-Based Storage Management Service	No	No
CVE-2024-26186 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-26191 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37335 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37337 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37338 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37339 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37340 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37342 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37966 SQL Server	SQL Server Native Scoring	No	No
CVE-2024-37341 SQL Server	SQL Server	No	No

CVE	Component	Public	Exploited
CVE-2024-37965 SQL Server	SQL Server	No	No
CVE-2024-37980 SQL Server	SQL Server	No	No
CVE-2024-43474 SQL Server	SQL Server	No	No
CVE-2024-38018 Microsoft Office SharePoint	SharePoint Server	No	No
CVE-2024-38227 Microsoft Office SharePoint	SharePoint Server	No	No
CVE-2024-38228 Microsoft Office SharePoint	SharePoint Server	No	No
CVE-2024-43464 Microsoft Office SharePoint	SharePoint Server	No	No
CVE-2024-43466 Microsoft Office SharePoint	SharePoint Server	No	No
CVE-2024-43457 Windows Setup and Deployment	Setup and Deployment	No	No
CVE-2024-30073 Windows Security Zone Mapping	Security Zone Mapping	No	No
CVE-2024-38231 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-38258 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-38260 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-38263 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-43454 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-43455 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No

CVE	Component	Public	Exploited
CVE-2024-43467 Windows Remote Desktop Licensing Service	Remote Desktop Licensing Service	No	No
CVE-2024-38240 Windows Remote Access Connection Manager	Remote Access Connection Manager	No	No
CVE-2024-38226 Microsoft Office Publisher	Publisher Security Features Bypass	No	Yes
CVE-2024-43479 Power Automate	Power Automate Desktop	No	No
CVE-2024-43482 Microsoft Outlook for iOS	Outlook for iOS	No	No
CVE-2024-43463 Microsoft Office Visio	Office Visio	No	No
CVE-2024-38232 Windows Network Virtualization	Networking	No	No
CVE-2024-38233 Windows Network Virtualization	Networking	No	No
CVE-2024-38234 Windows Network Virtualization	Networking	No	No
CVE-2024-43458 Windows Network Virtualization	Networking	No	No
CVE-2024-38119 Windows Network Address Translation (NAT)	Network Address Translation (NAT)	No	No
CVE-2024-43461 Windows MSHTML Platform	MSHTML Platform	No	No
CVE-2024-38217 Windows Mark of the Web (MOTW)	Mark of the Web	Yes	Yes
CVE-2024-43487 Windows Mark of the Web (MOTW)	Mark of the Web	No	No
CVE-2024-38259 Microsoft Management Console	Management Console	No	No
CVE-2024-43495 Windows Libarchive	libarchive	No	No

CVE	Component	Public	Exploited
CVE-2024-38256 Windows Kernel-Mode Drivers	Kernel-Mode Driver	No	No
CVE-2024-38239 Windows Kerberos	Kerberos	No	No
CVE-2024-38014 Windows Installer	Installer	No	Yes
CVE-2024-38235 Role: Windows Hyper-V	Hyper-V	No	No
CVE-2024-38247 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-38249 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-38250 Microsoft Graphics Component	Graphics Component	No	No
CVE-2024-43465 Microsoft Office Excel	Excel	No	No
CVE-2024-38225 Dynamics Business Central	Dynamics 365 Business Central	No	No
CVE-2024-43476 Microsoft Dynamics 365 (on-premises)	Dynamics 365 (on-premises) Cross-site Scripting	No	No
CVE-2024-43492 Microsoft AutoUpdate (MAU)	AutoUpdate (MAU)	No	No
CVE-2024-38254 Windows Authentication Methods	Authentication	No	No
CVE-2024-38257 Windows AllJoyn API	AllJoyn API	No	No