Microsoft

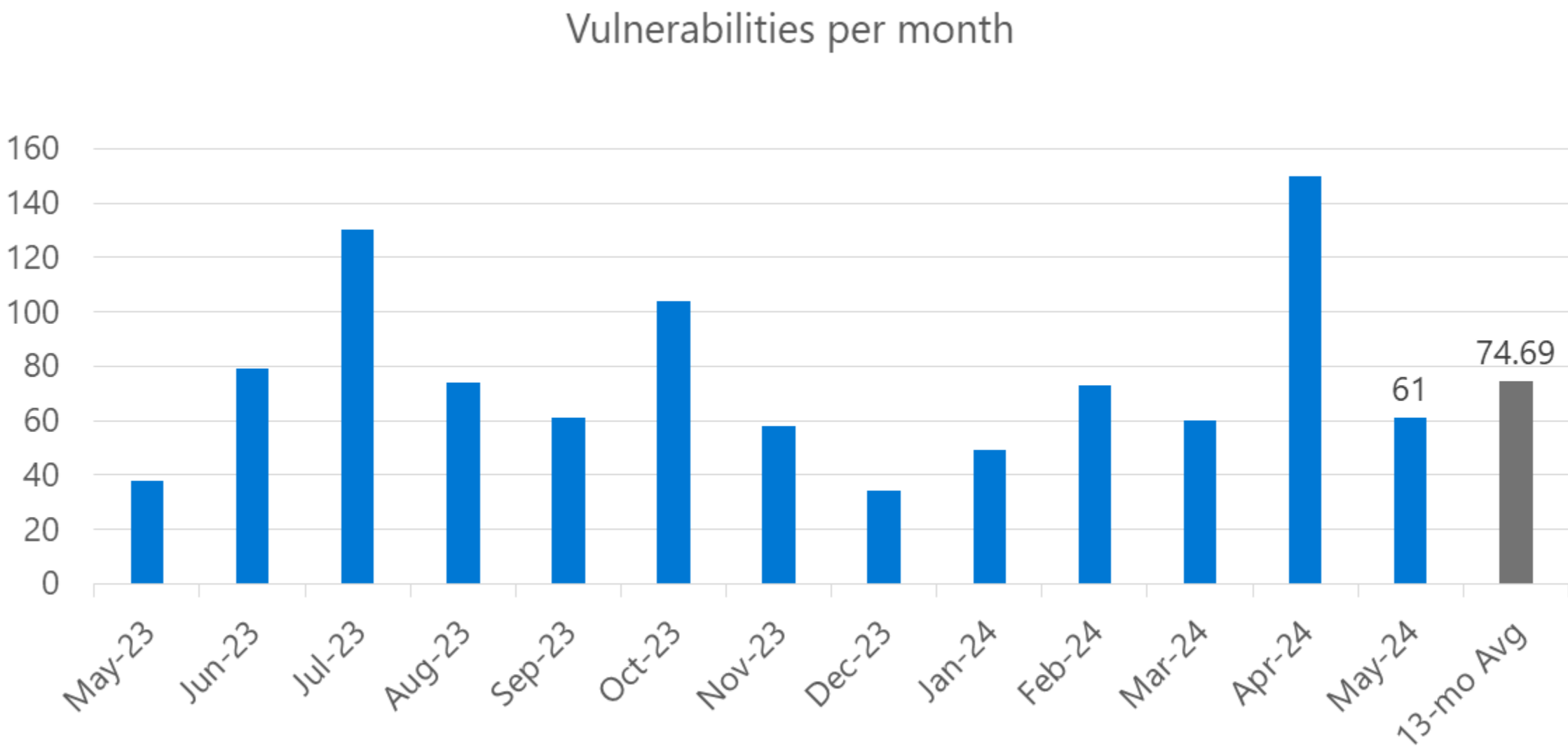
Microsoft Security Release

May 14, 2024

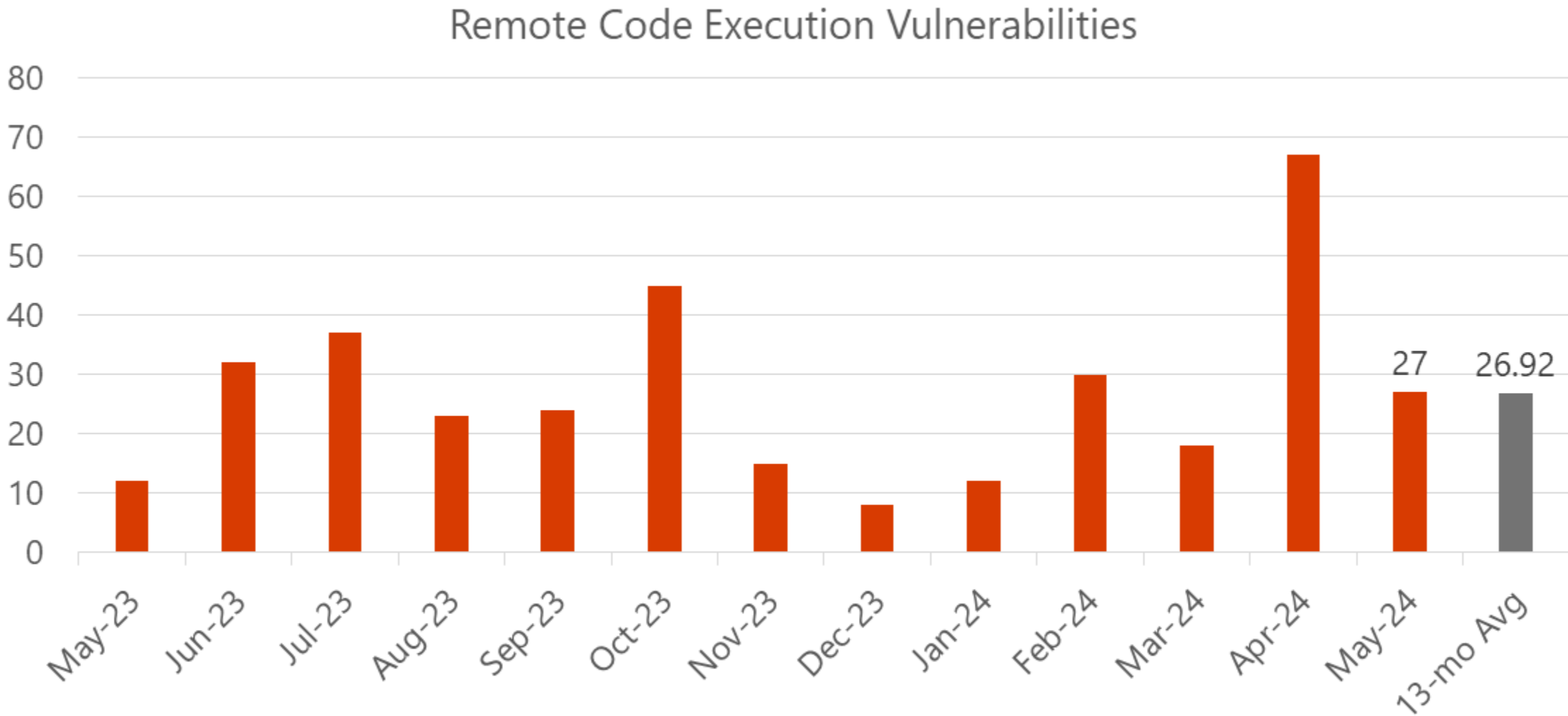
Agenda

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

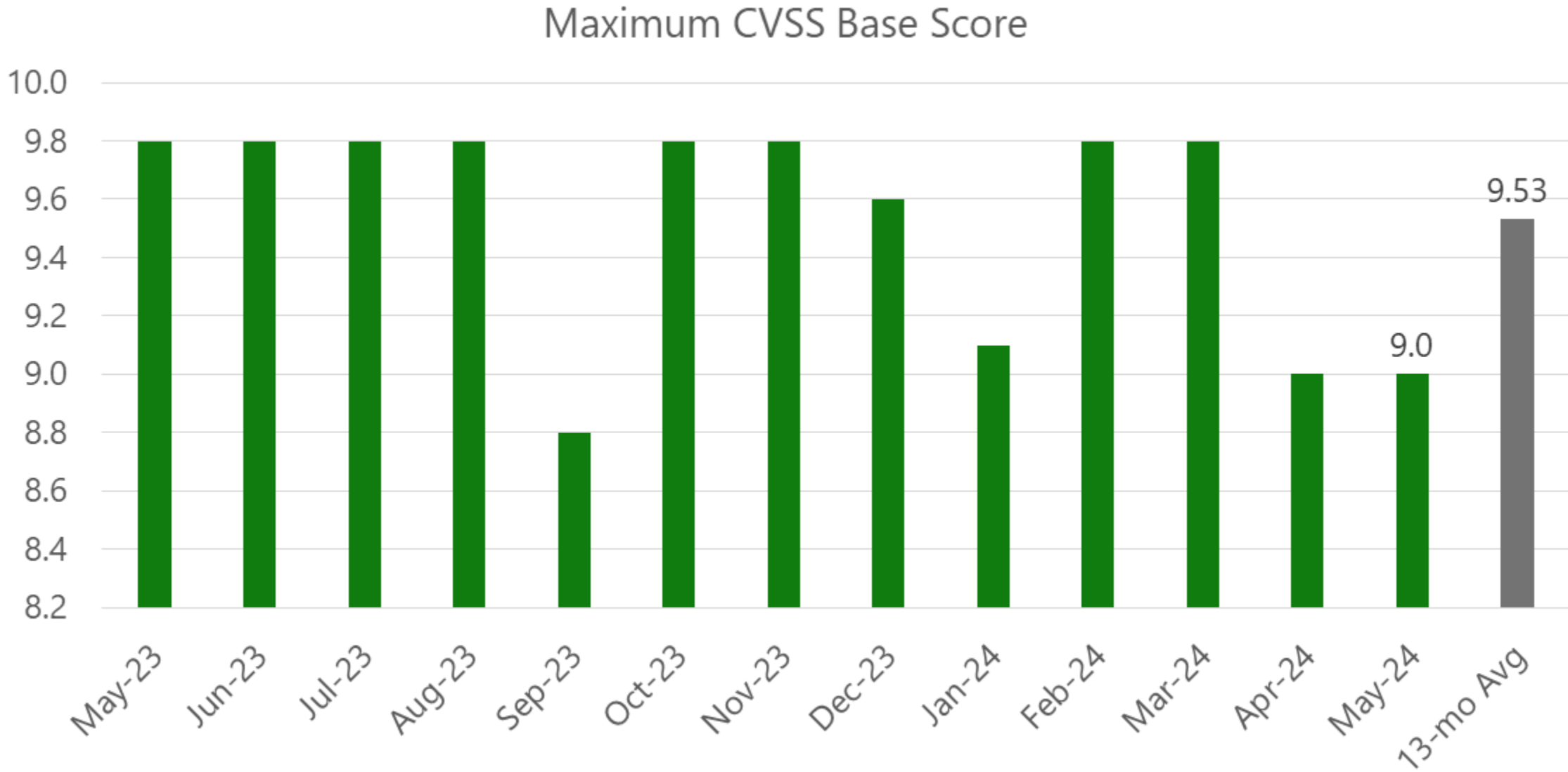
Microsoft


Vulnerabilities per month
160
140
120
100
80
60
40
20
0
61
74.69
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
13-mo Avg

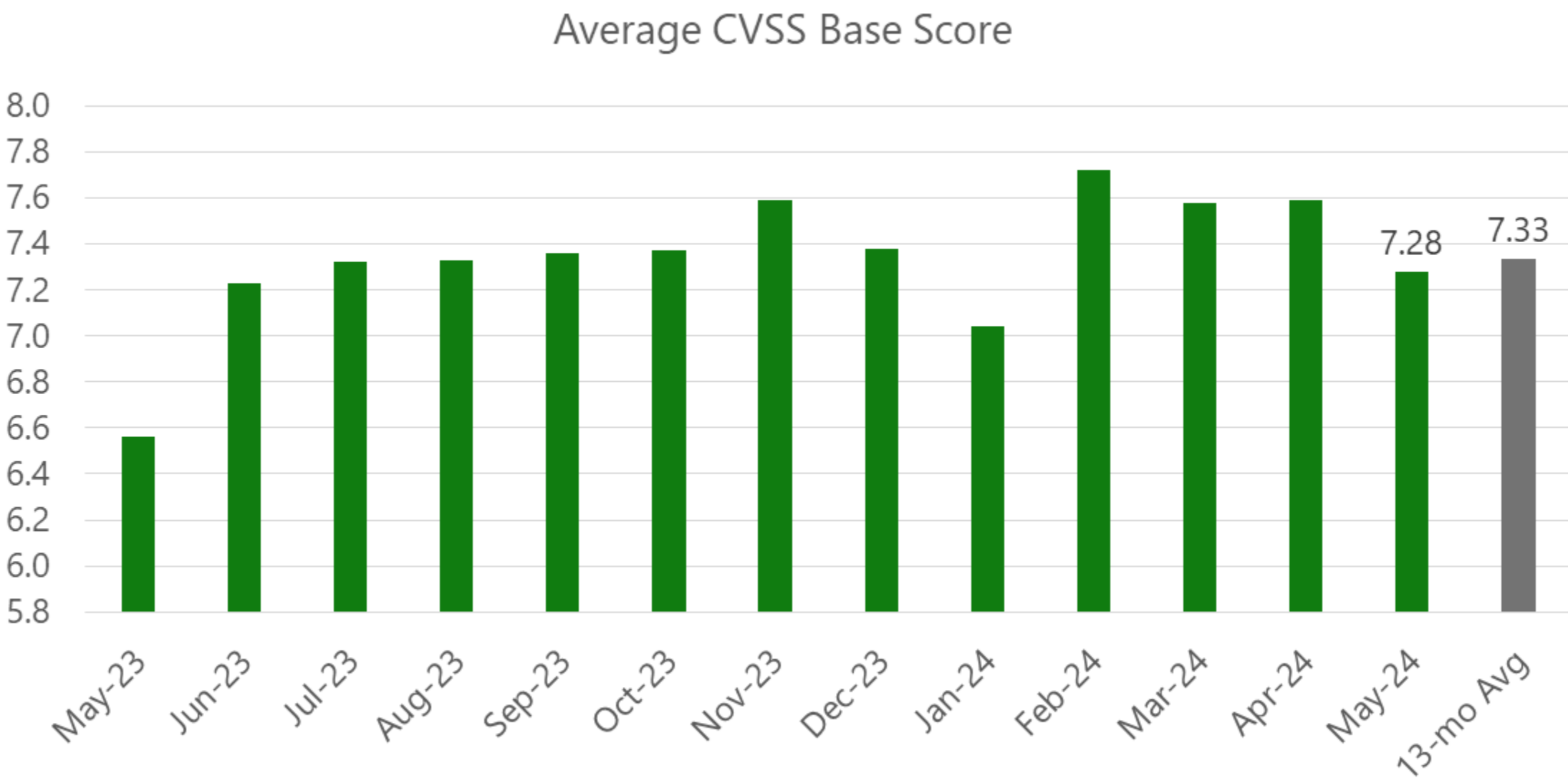
Microsoft


Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
27
26.92
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
13-mo Avg

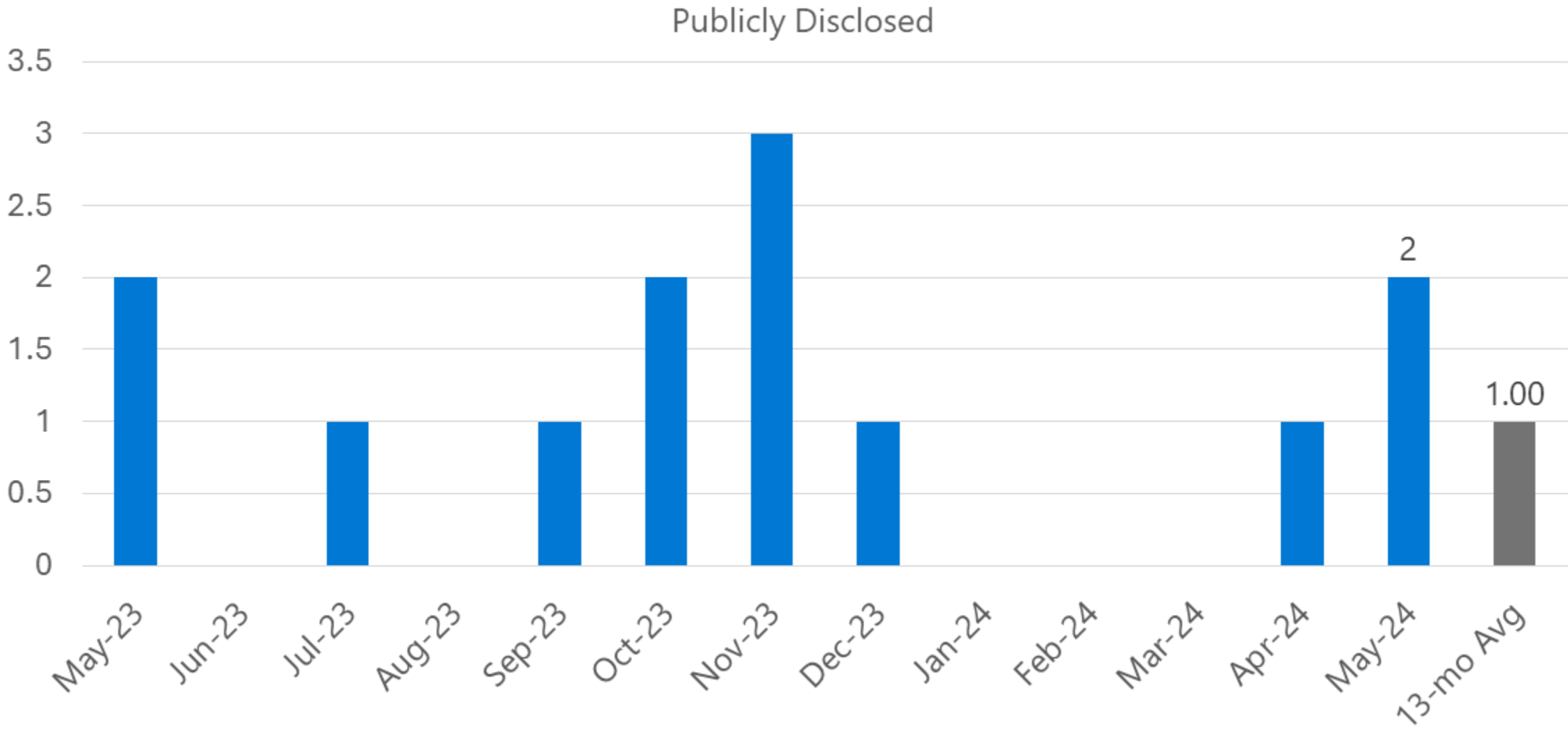
Microsoft


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

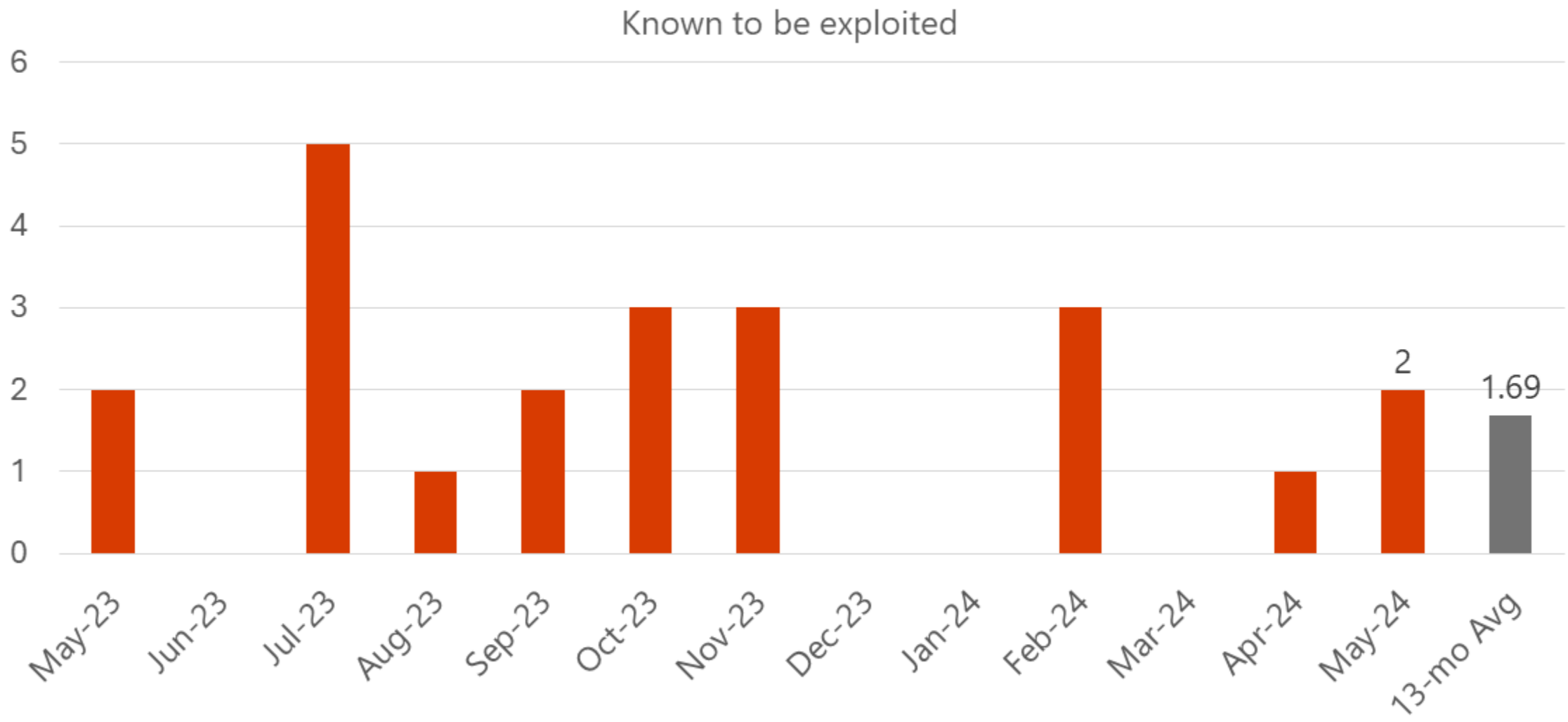
Microsoft


Average CVSS Base Score
8.0
7.8
7.6
7.4
7.2
7.0
6.8
6.6
6.4
6.2
6.0
5.8
7.28
7.33
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
13-mo Avg

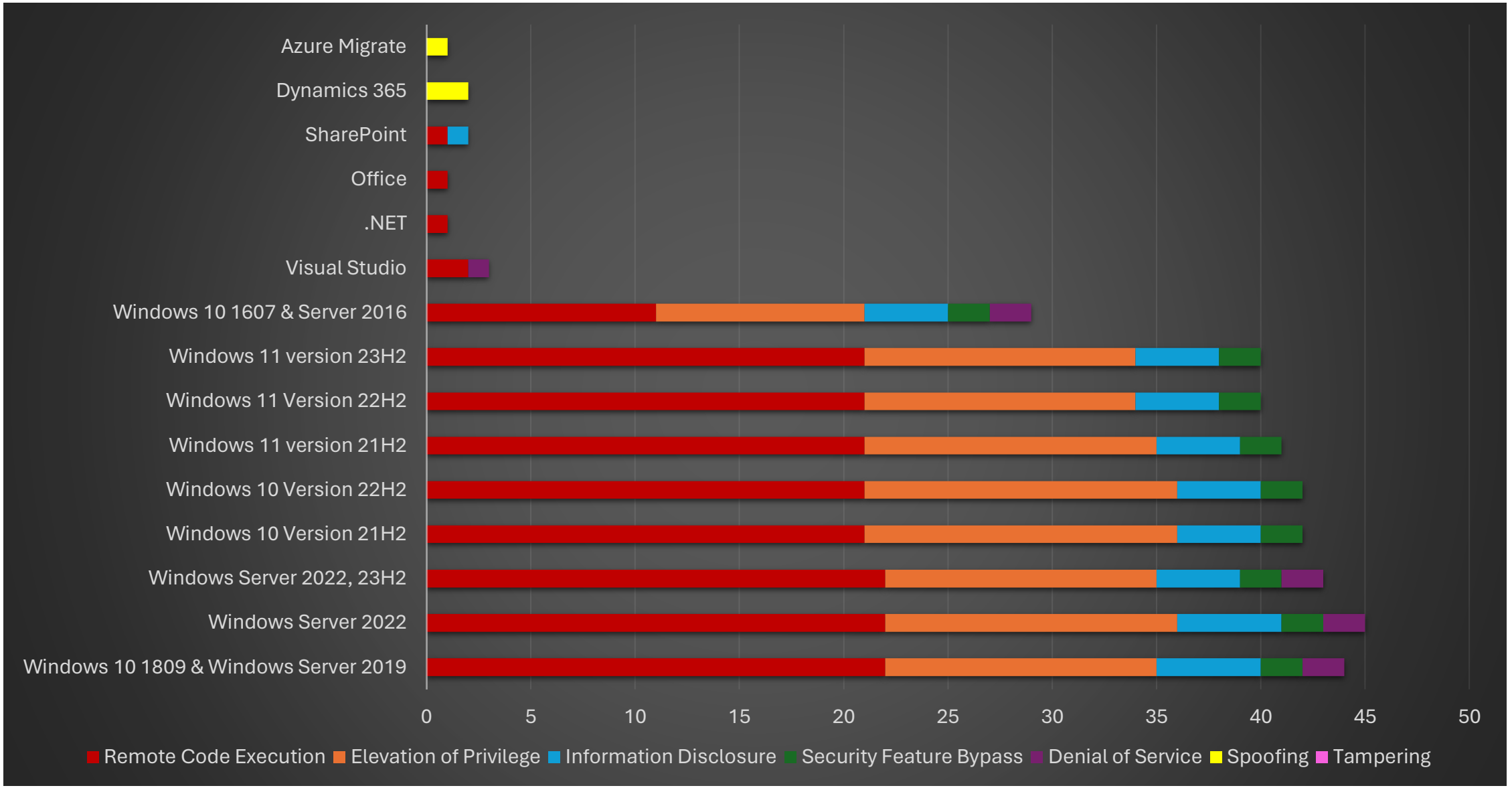
Microsoft


Publicly Disclosed
3.5
3
2.5
2
1.5
1
0.5
0
2
1.00
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
13-mo Avg

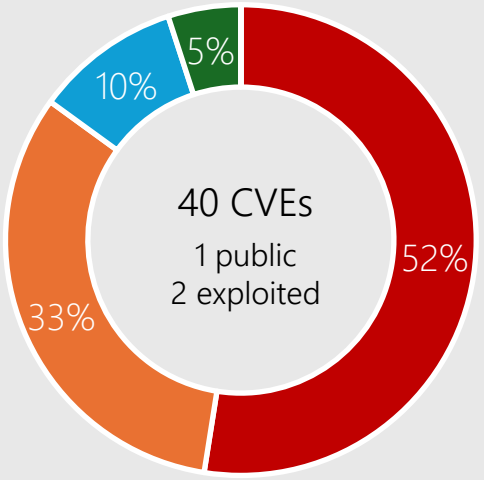
Microsoft


Known to be exploited
6
5
4
3
2
1
0
2
1.69
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
13-mo Avg

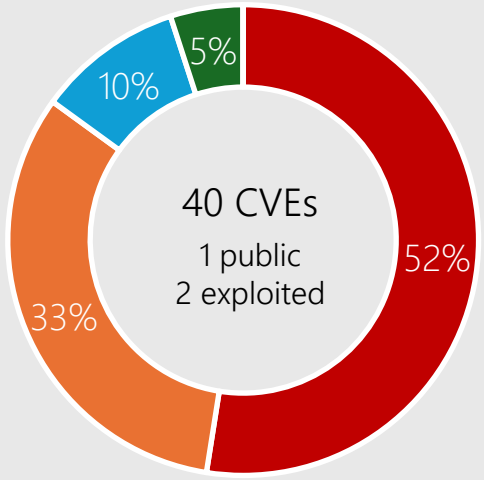
Microsoft Security Release Overview – May 2024



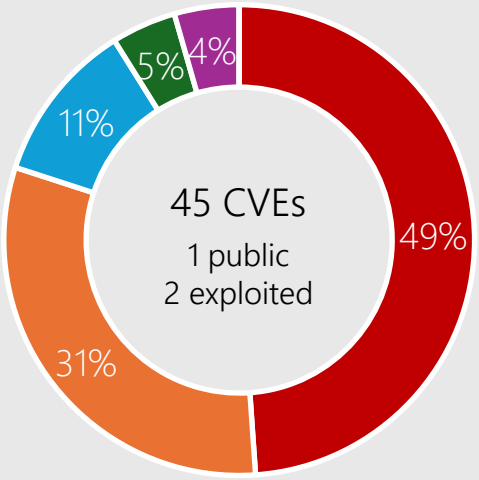
Windows 11, Server 2022



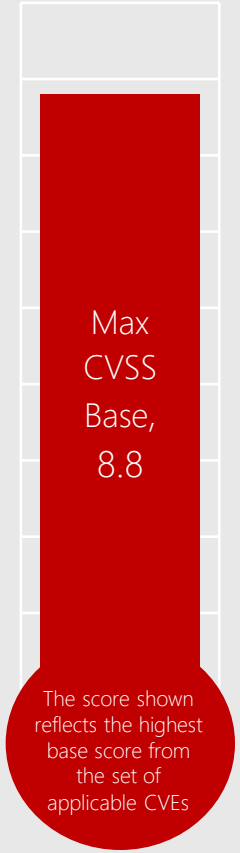
Windows 11 23H2



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-2024-30051 DWM Core Library

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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-2024-30040 MSHTML

Impact, Severity, Disclosure

Security Feature Bypass | 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 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-2024-30017 Hyper-V

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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-30007 Brokering File System

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

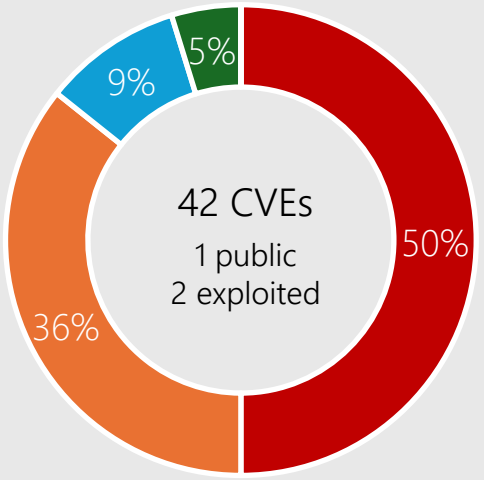
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

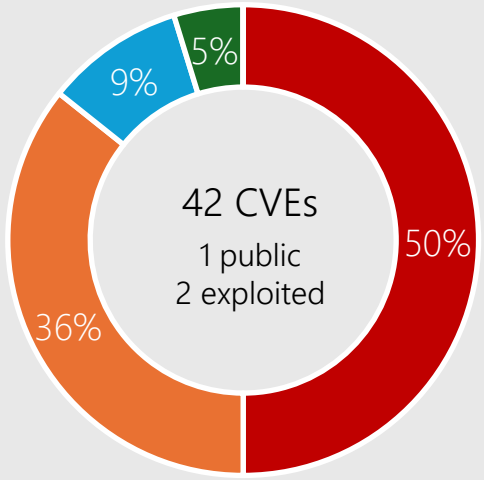
Affected Software

Server 2022, 23H2

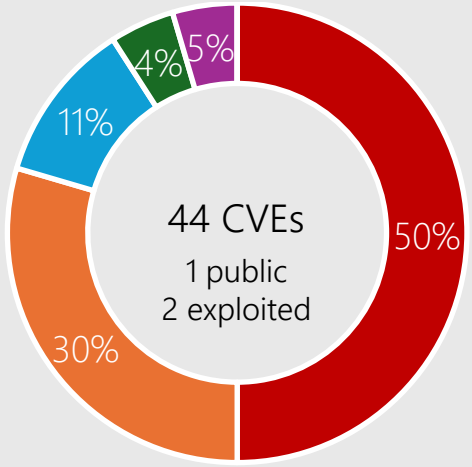
Windows 10



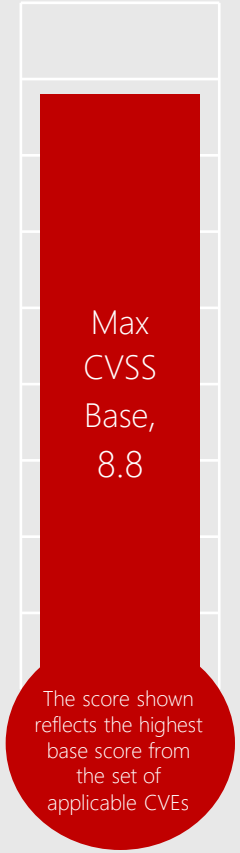
Windows 10 22H2



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-2024-30009 RRAS

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-2024-30006 WDAC OLE DB 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-2024-30020 Cryptographic Services

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.

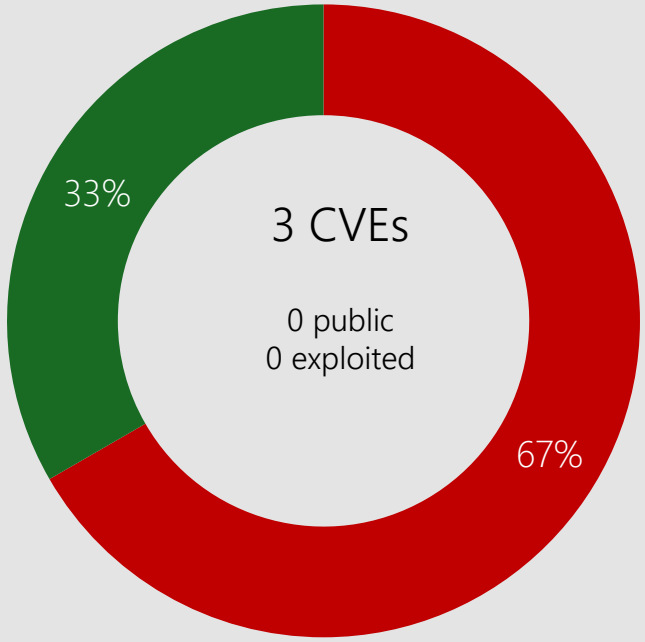
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

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

Products:

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

CVE-2024-30044 SharePoint Server

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 Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

CVE-2024-30042 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 LTSC for Mac 2021
Office LTSC 2021
Excel 2016
Office Online Server
Office 2019
365 Apps Enterprise

Other Products

Dynamics 365

CVE-2024-30047 | 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 Customer Insights

CVE-2024-30048 | 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 Customer Insights

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-30045 | .NET and Visual Studio Remote Code Execution Vulnerability

Base CVSS: 6.3 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: Required
Affected Products: .NET 7.0, .NET 8.0, Visual Studio 2022

CVE-2024-30046 | Visual Studio Denial of Service Vulnerability

Base CVSS: 5.9 | **Max Severity**: Important | **Public**: Yes | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Visual Studio 2022

Developer Tools

Visual Studio

CVE-2024-32002 | MinGit Remote Code Execution Vulnerability

Base CVSS: 9.0 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Visual Studio 2017

CVE-2024-32004 | MinGit Remote Code Execution Vulnerability

Base CVSS: 8.1 **| Max Severity:** Important **| Public:** No **| Exploited:** No
Attack Vector: Local **| Attack Complexity:** High **| Privileges Required:** None **| User Interaction Required:** None
Affected Products: Visual Studio 2022, Visual Studio 2019, Visual Studio 2017

Other Products

Azure Migrate

CVE-2024-30053 | Important | Spoofing| Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure Migrate

Other Products

Apps

CVE-2024-30041 Bing Search for iOS
CVE-2024-30054 Power BI-client JS SDK
CVE-2024-30059 Intune Mobile Application Mgmt for Android

Product Lifecycle Update

Modern Policy

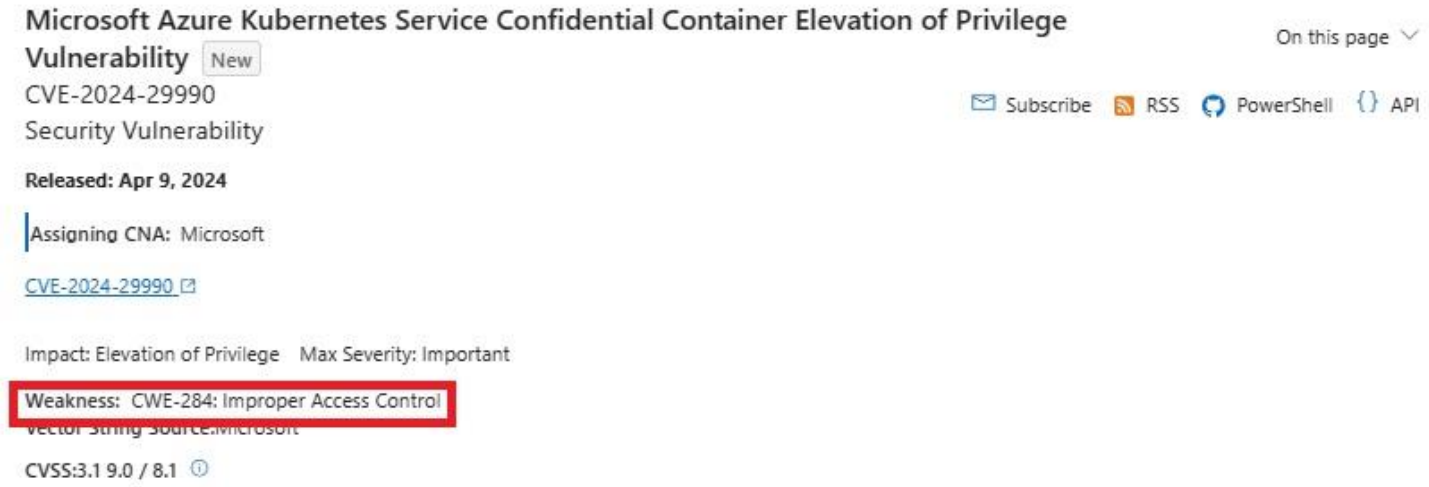
.NET 7

Coming June 11, 2024

Windows 10 21H2 (Ent and EDU)

Latest Servicing Stack Updates

Toward greater transparency: Adopting the CWE standard for Microsoft CVEs



- Link to MSRC Blog:[Toward greater transparency: Adopting the CWE standard for Microsoft CVEs | MSRC Blog | Microsoft Security Response Center]

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2024-29996	No	No	Common Log File System Driver
CVE-2024-29997	No	No	Mobile Broadband Driver
CVE-2024-29998	No	No	Mobile Broadband Driver
CVE-2024-29999	No	No	Mobile Broadband Driver
CVE-2024-30000	No	No	Mobile Broadband Driver
CVE-2024-30001	No	No	Mobile Broadband Driver
CVE-2024-30002	No	No	Mobile Broadband Driver
CVE-2024-30003	No	No	Mobile Broadband Driver
CVE-2024-30004	No	No	Mobile Broadband Driver
CVE-2024-30005	No	No	Mobile Broadband Driver
CVE-2024-30008	No	No	DWM Core Library
CVE-2024-30009	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30010	No	No	Hyper-V
CVE-2024-30011	No	No	Hyper-V

CVE	Public	Exploited	Product
CVE-2024-30012	No	No	Mobile Broadband Driver
CVE-2024-30014	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30015	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30016	No	No	Cryptographic Services
CVE-2024-30017	No	No	Hyper-V
CVE-2024-30018	No	No	Kernel
CVE-2024-30019	No	No	DHCP Server Service
CVE-2024-30020	No	No	Cryptographic Services
CVE-2024-30021	No	No	Mobile Broadband Driver
CVE-2024-30022	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30023	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30050	No	No	Mark of the Web
CVE-2024-26238	No	No	PLUGScheduler Scheduled Task
CVE-2024-29994	No	No	SCSI Class System File

CVE	Public	Exploited	Product
CVE-2024-30024	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30025	No	No	Common Log File System Driver
CVE-2024-30027	No	No	NTFS
CVE-2024-30028	No	No	Win32k
CVE-2024-30029	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30030	No	No	Win32k
CVE-2024-30031	No	No	CNG Key Isolation Service
CVE-2024-30032	No	No	DWM Core Library
CVE-2024-30033	No	No	Search Service
CVE-2024-30034	No	No	Cloud Files Mini Filter Driver
CVE-2024-30035	No	No	DWM Core Library
CVE-2024-30036	No	No	Deployment Services
CVE-2024-30037	No	No	Common Log File System Driver
CVE-2024-30038	No	No	Win32k

CVE	Public	Exploited	Product
CVE-2024-30039	No	No	Remote Access Connection Manager
CVE-2024-30040	No	Yes	MSHTML Platform
CVE-2024-30049	No	No	Win32 Kernel Subsystem
CVE-2024-30051	Yes	Yes	DWM Core Library
CVE-2024-4331	No	No	Chromium: CVE-2024-4331 Use after free in Picture In Picture
CVE-2024-4368	No	No	Chromium: CVE-2024-4368 Use after free in Dawn
CVE-2024-30044	No	No	SharePoint Server
CVE-2024-30042	No	No	Excel
CVE-2024-30043	No	No	SharePoint Server
CVE-2024-32002	No	No	CVE-2023-32002 Recursive clones on case-insensitive filesystems that support symlinks are susceptible to
CVE-2024-30006	No	No	WDAC OLE DB provider for SQL Server
CVE-2024-30007	No	No	Brokering File System
CVE-2024-30053	No	No	Azure Migrate Cross-Site Scripting
CVE-2024-30059	No	No	Intune for Android Mobile Application Management

CVE	Public	Exploited	Product
CVE-2024-30041	No	No	Bing Search
CVE-2024-30045	No	No	.NET and Visual Studio
CVE-2024-30046	Yes	No	ASP.NET Core
CVE-2024-30047	No	No	Dynamics 365 Customer Insights
CVE-2024-30048	No	No	Dynamics 365 Customer Insights
CVE-2024-32004	No	No	GitHub: CVE-2023-32004 while cloning special-crafted local repositories
CVE-2024-30054	No	No	Power BI Client Javascript SDK