Microsoft

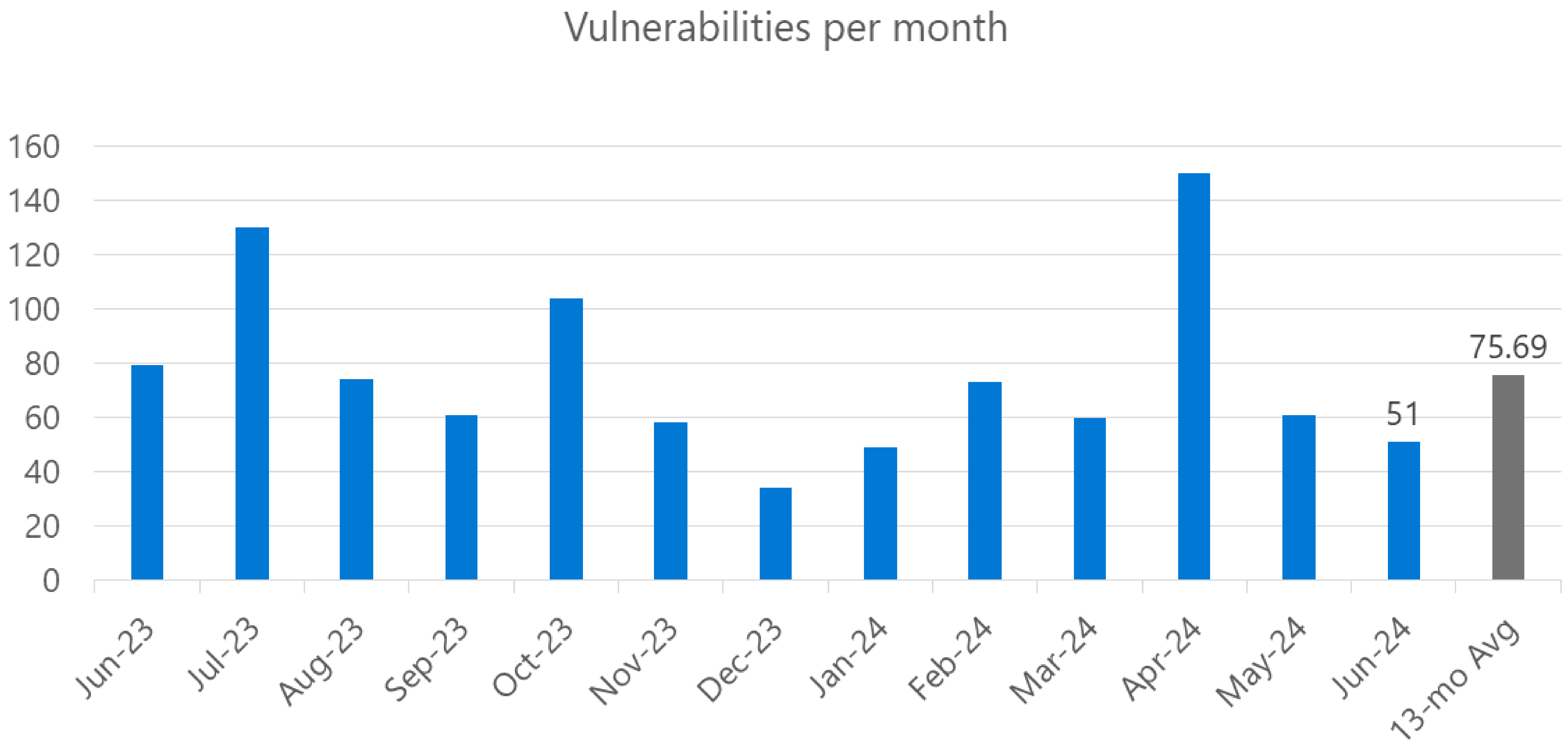
Microsoft Security Release

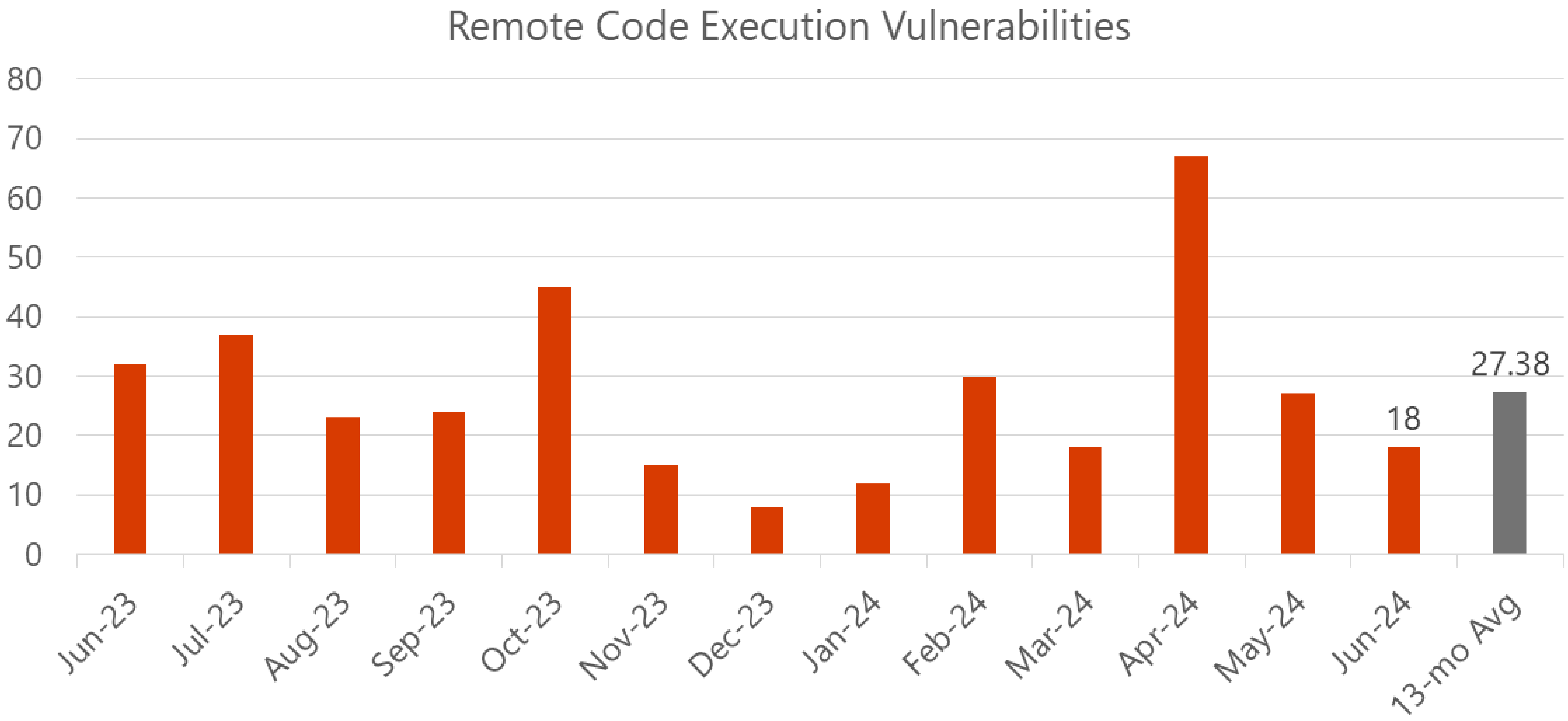
June 11, 2024

Agenda

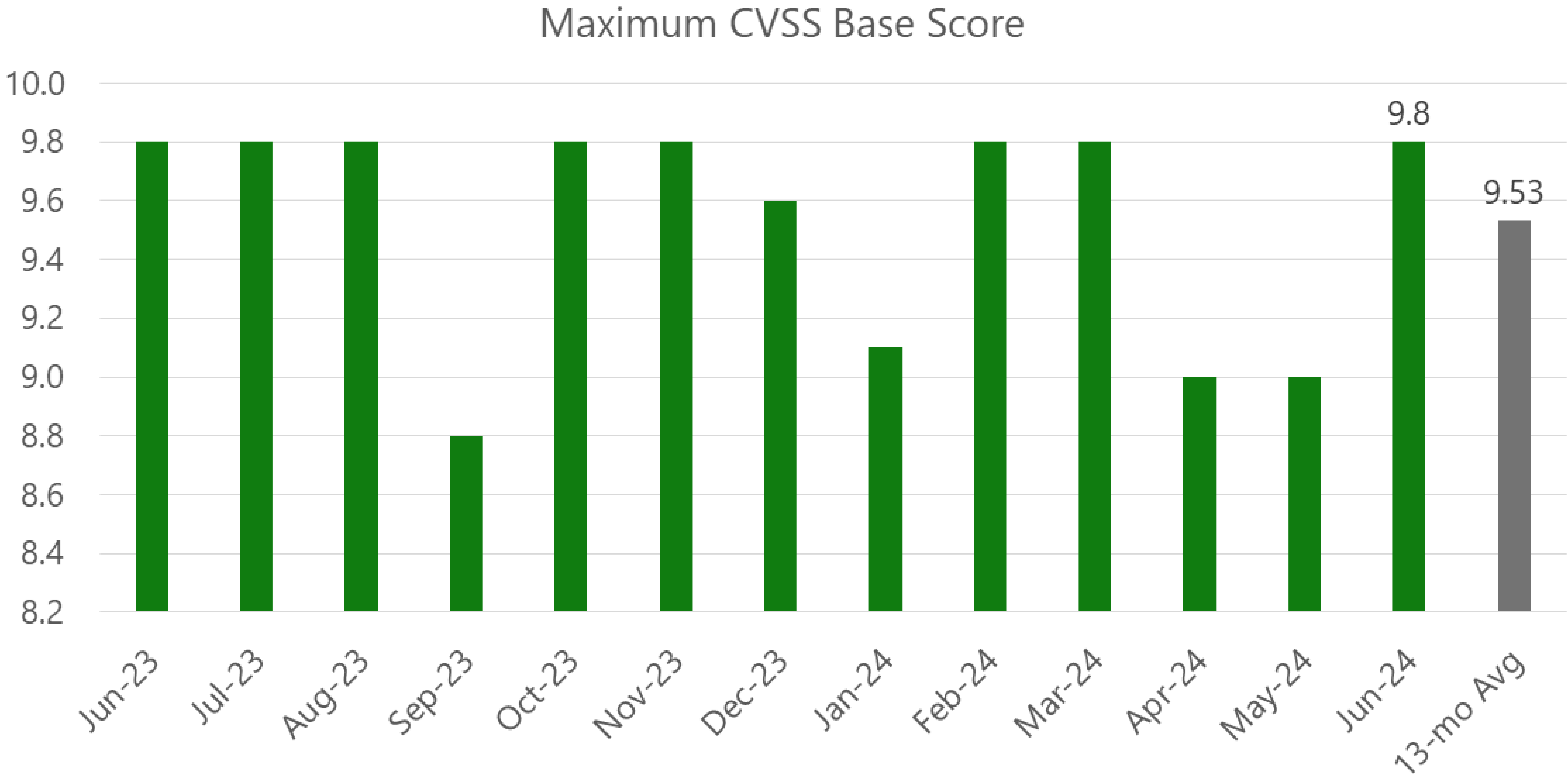
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

Microsoft


Vulnerabilities per month
160
140
120
100
80
60
40
20
0
75.69
51
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
13-mo Avg

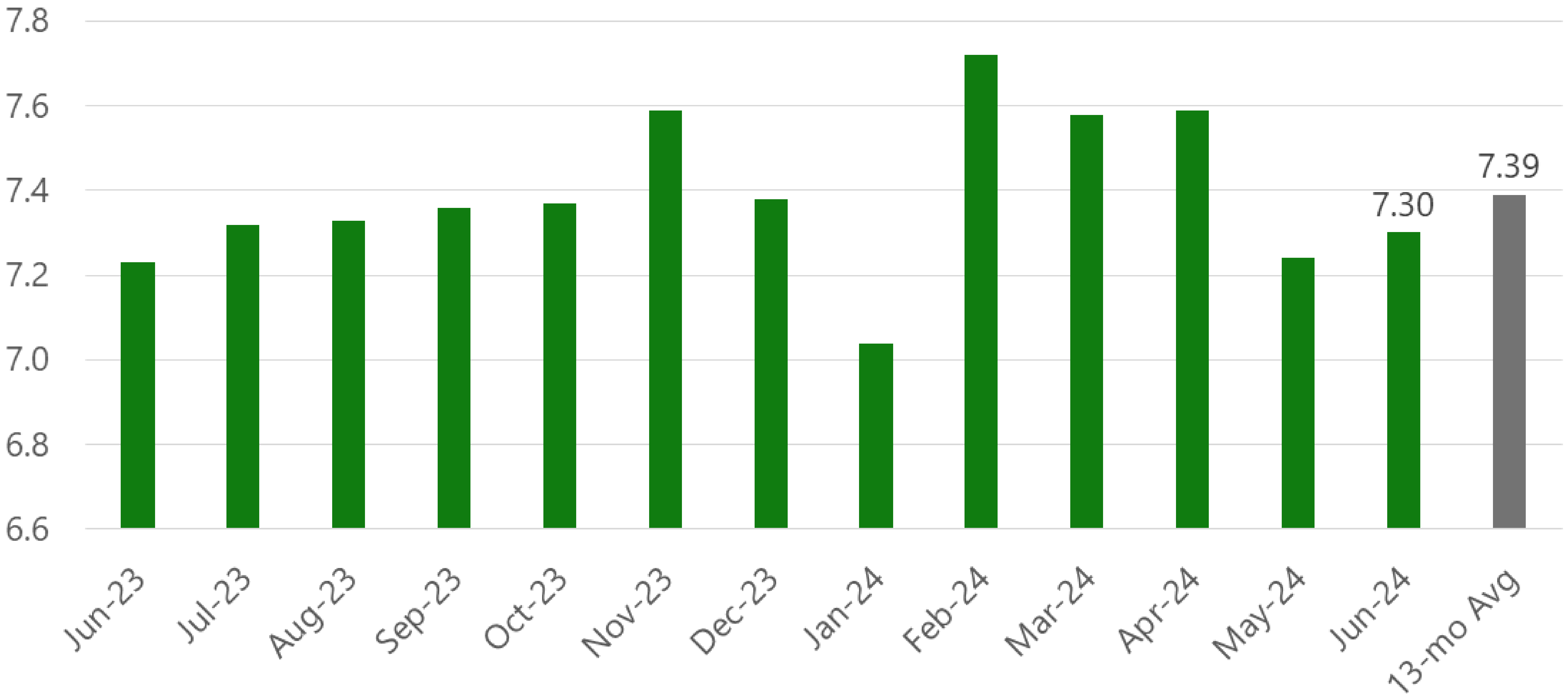

Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
13-mo Avg
18
27.38

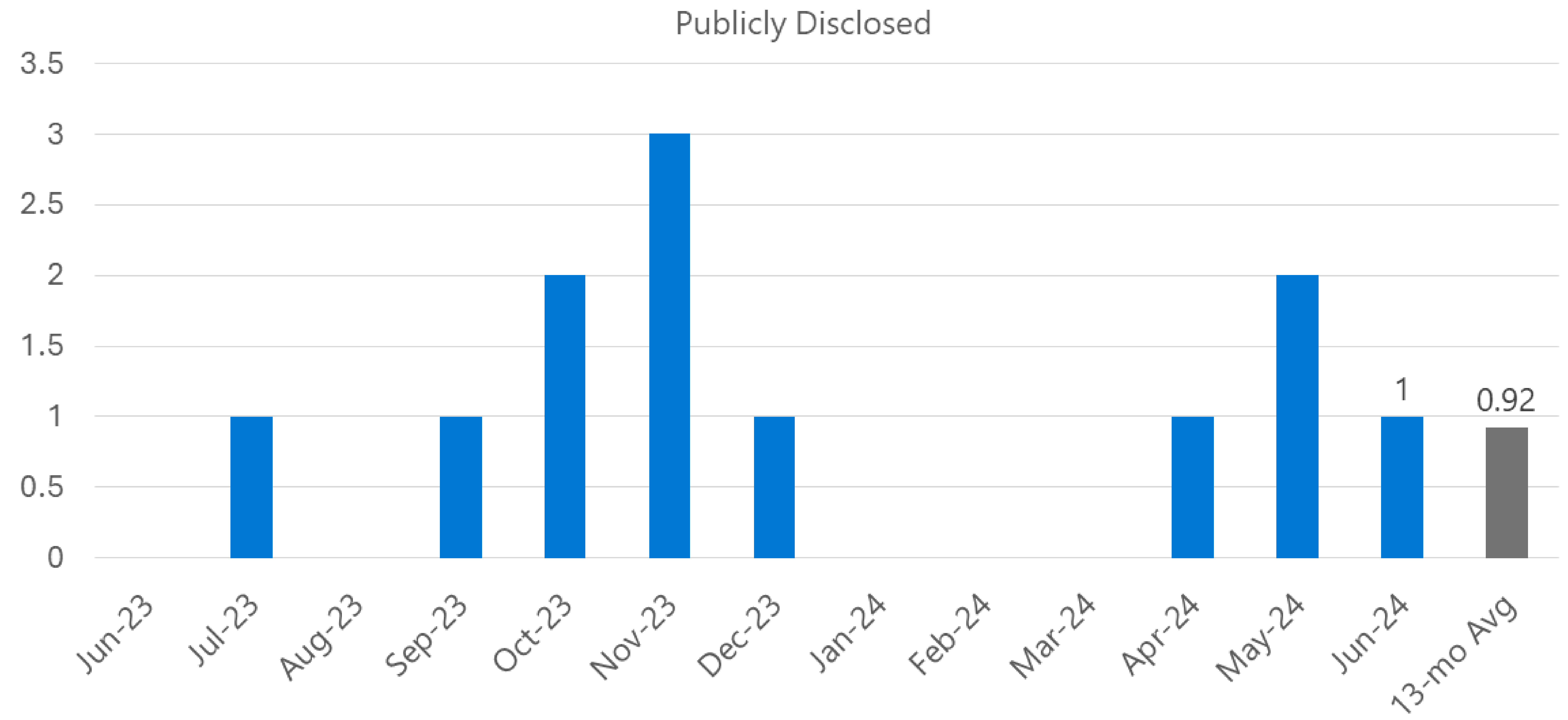
Microsoft


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

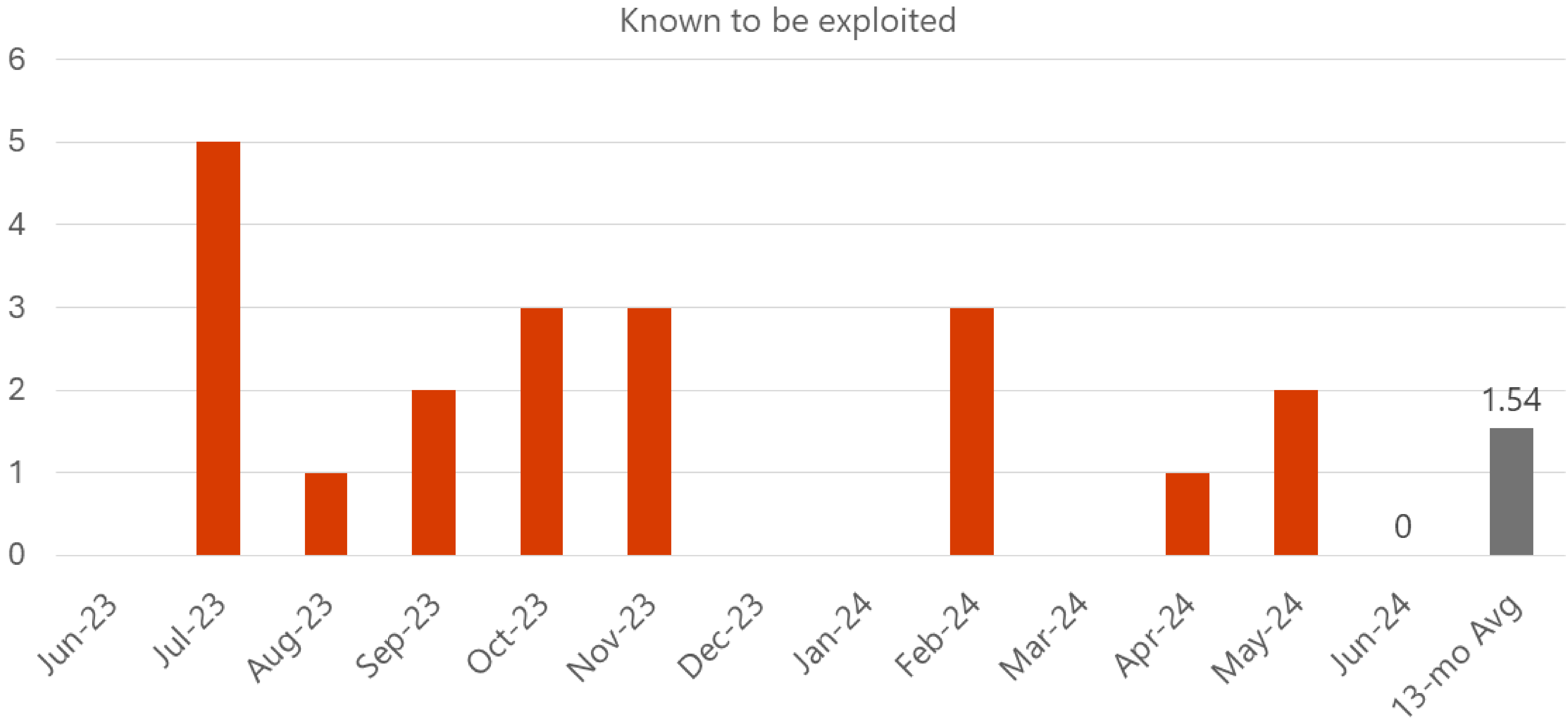
Microsoft

Average CVSS Base Score

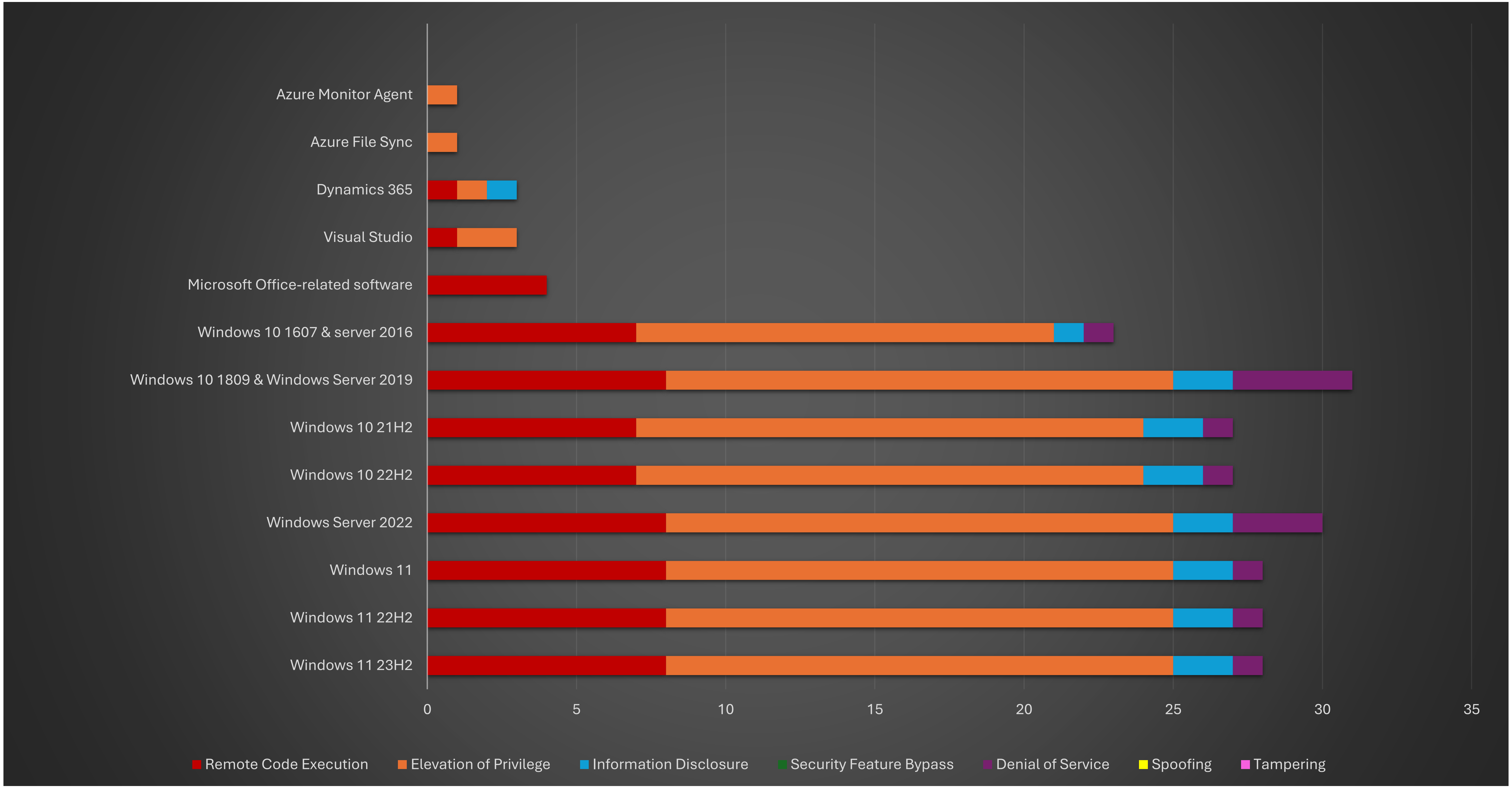



Publicly Disclosed
3.5
3
2.5
2
1.5
1
0.5
0
1
0.92
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
13-mo Avg

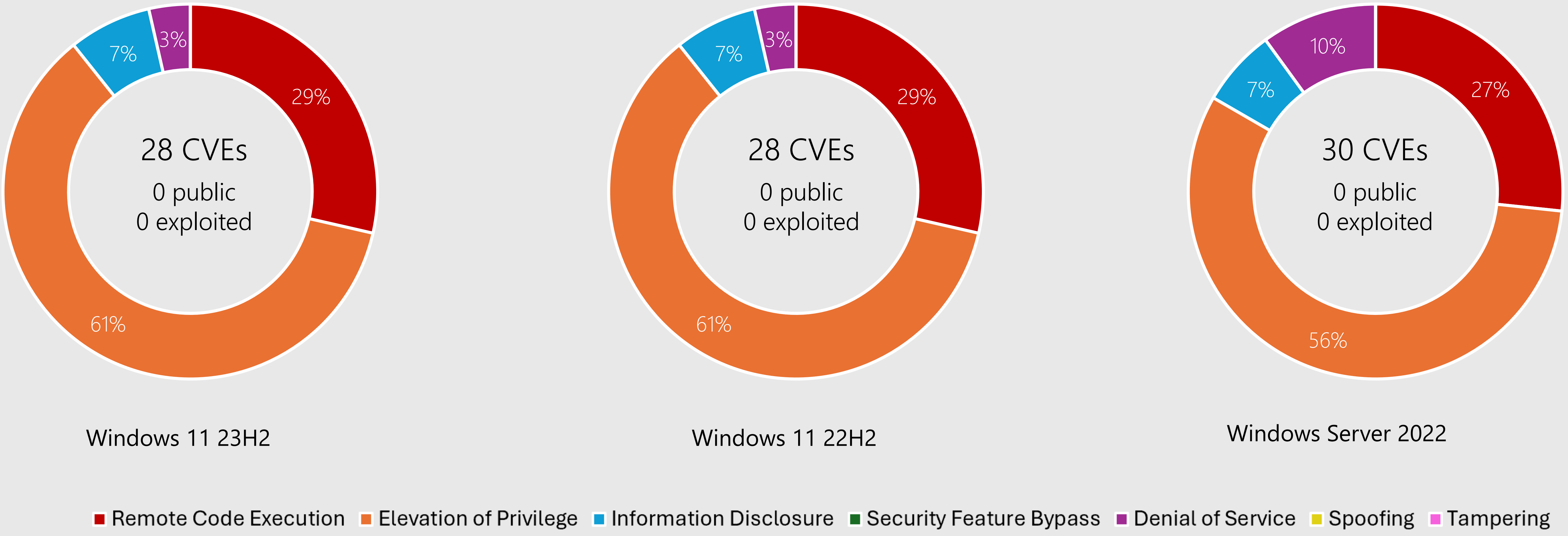
Microsoft

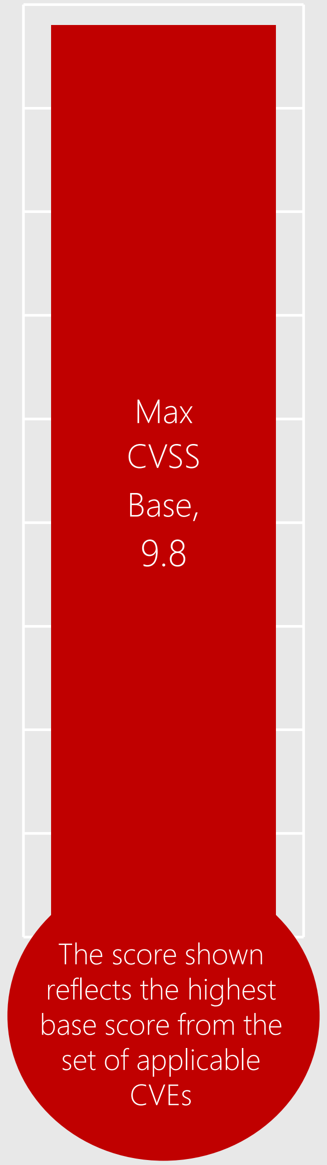

Known to be exploited
6
5
4
3
2
1
0
1.54
0
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
13-mo Avg

Microsoft Security Release Overview – June 2024



Windows 11, Server 2022





Max CVSS Base, 9.8

The score shown reflects the highest base score from the set of applicable CVEs

Affected Components:

See Appendix for details

CVE-2024-30080 Message Queuing (MSMQ)

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

The Windows message queuing service, which is a Windows component, needs to be enabled for a system to be exploitable by this vulnerability. This feature can be added via the Control Panel.

You can check to see if there is a service running named Message Queuing and TCP port 1801 is listening on the machine.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-30078 Wi-Fi Driver

Impact, Severity, Disclosure

Remote Code Execution | Important | 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-2024-30097 SAPI

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.

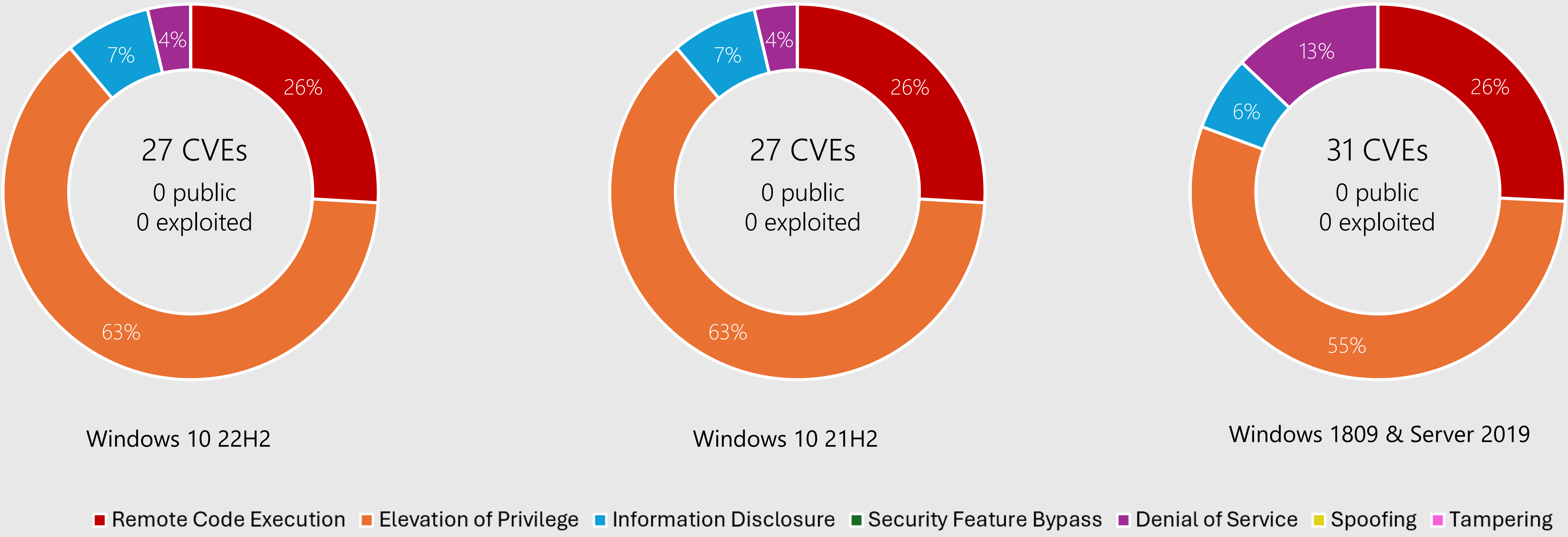
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Windows 10



Max CVSS Base, 9.8

The score shown reflects the highest base score from the set of applicable CVEs

Affected Components:

See Appendix for details

CVE-2024-30077 OLE

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8 | Attack Vector: Network | 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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-30068 Kernel

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.

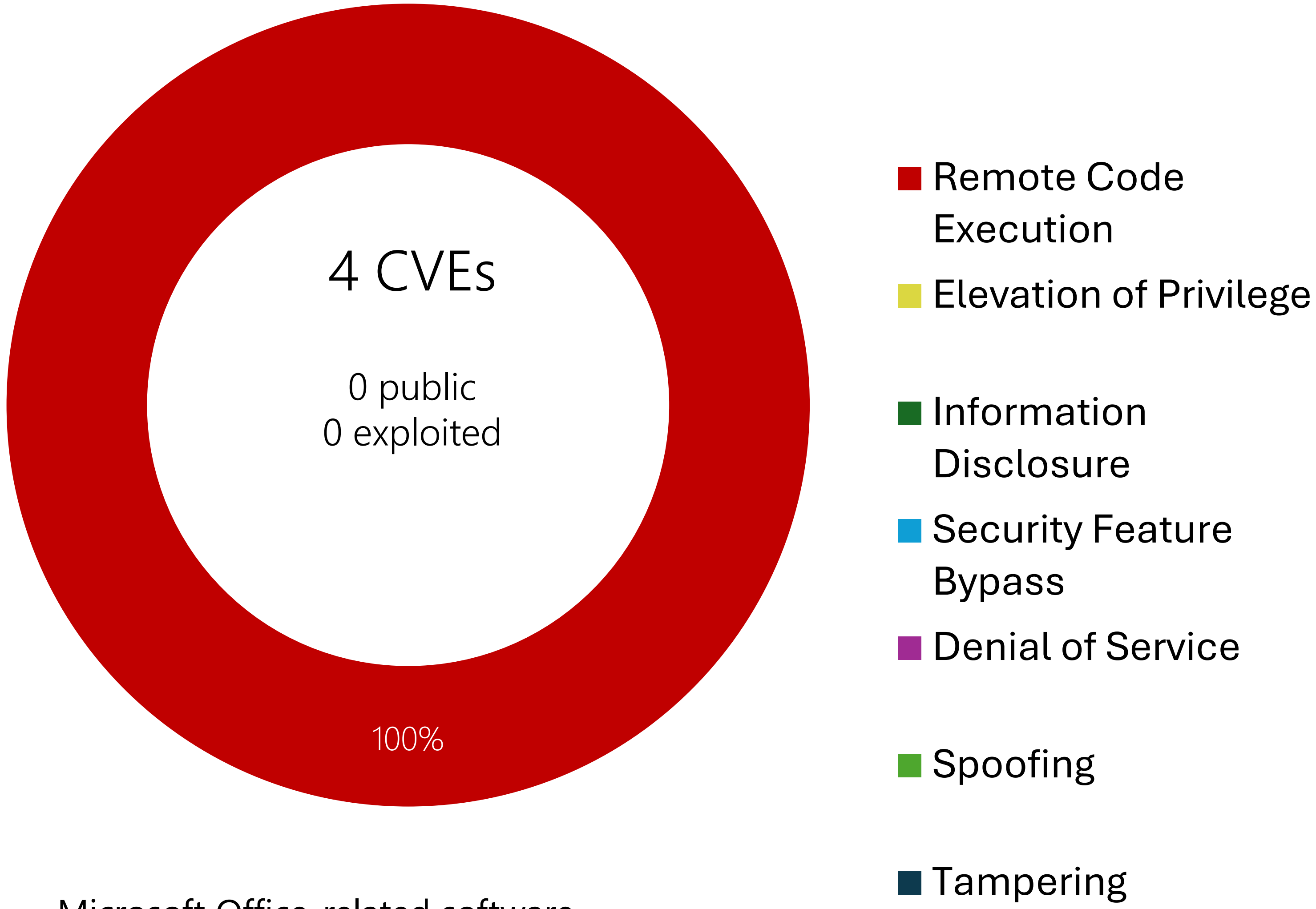
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

Office 2016/2019
Outlook 2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office LTSC 2021
SharePoint Server Subscription Edition

CVE-2024-30100 SharePoint Server

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

SharePoint Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

CVE-2024-30103 Outlook

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

Office LTSC 2021
Outlook 2016
Office 2019
365 Apps Enterprise

CVE-2024-30104 Office

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 2021
Office 2016
Office 2019
365 Apps Enterprise

Other Products

Dynamics 365

CVE-2024-35248 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Dynamics 365 Business Central 2024 Release Wave 1, Dynamics 365 Business Central 2023 Release Wave 2, Dynamics 365 Business Central 2023 Release Wave 1.

CVE-2024-35249 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 Business Central 2023 Release Wave 2, Dynamics 365 Business Central 2023 Release Wave 1, Dynamics 365 Business Central 2024 Release Wave 1.

Other Products

Dynamics 365

CVE-2024-35263 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.7
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1.

Other Products

Visual Studio

CVE-2024-29060 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.7
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.8, Visual Studio 2022 version 17.10, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2024-29187 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.8, Visual Studio 2022 version 17.10, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4.

Other Products

Visual Studio

CVE-2024-30052 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 4.7
Attack Vector: Local
Attack Complexity: High
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.8, Visual Studio 2022 version 17.10, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4.

Other Products

Azure Data Science Virtual Machines for Linux

CVE-2024-37325 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Azure Data Science Virtual for Machines Linux.

Other Products

Azure Monitor Agent

CVE-2024-35254 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure Monitor Agent.

Other Products

Azure File Sync

CVE-2024-35253 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 4.4
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Azure File Sync v16.0, Azure File Sync v18.0, Azure File Sync v17.0.

Other Products

Azure

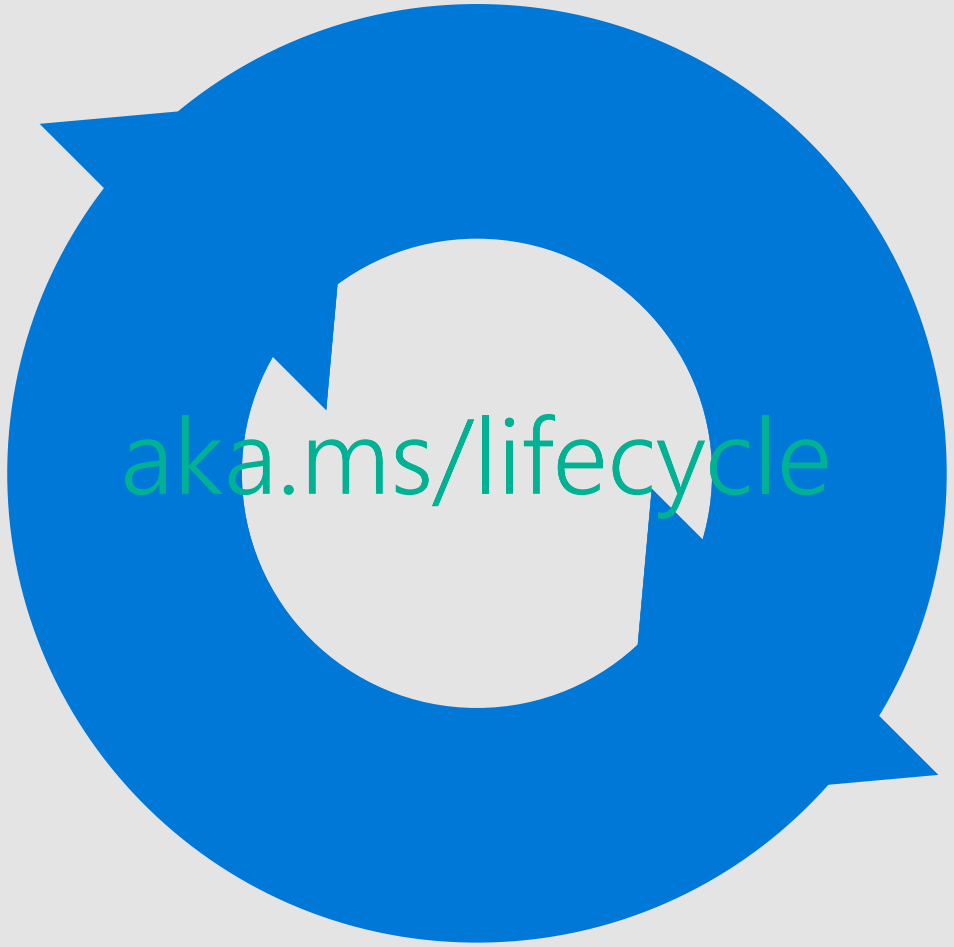
CVE-2024-35255 Azure Identity Library/ Microsoft Authentication Library

CVE-2024-35252 Azure Storage Movement Client Library for .NET

Product Lifecycle Update

Windows 10 Semi-Annual Channel
end of service

Windows 10 21H2



aka.ms/lifecycle

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2024-30069	No	No	Remote Access Connection Manager
CVE-2024-30070	No	No	DHCP Server Service
CVE-2024-30072	No	No	Event Trace Log File Parsing
CVE-2024-30074	No	No	Link Layer Topology Discovery Protocol
CVE-2024-30075	No	No	Link Layer Topology Discovery Protocol
CVE-2024-30076	No	No	Container Manager Service
CVE-2024-30077	No	No	OLE
CVE-2024-30078	No	No	Wi-Fi Driver
CVE-2024-30080	No	No	Message Queuing (MSMQ)
CVE-2024-30082	No	No	Win32k
CVE-2024-35250	No	No	Kernel-Mode Driver
CVE-2023-50868	Yes	No	MITRE: CVE-2023-50868
CVE-2024-30062	No	No	Standards-Based Storage Management Service
CVE-2024-30063	No	No	DFS

CVE	Public	Exploited	Product
CVE-2024-30064	No	No	Kernel
CVE-2024-30065	No	No	Themes
CVE-2024-30068	No	No	Kernel
CVE-2024-30083	No	No	Standards-Based Storage Management Service
CVE-2024-30084	No	No	Kernel-Mode Driver
CVE-2024-30085	No	No	Cloud Files Mini Filter Driver
CVE-2024-30086	No	No	Win32 Kernel Subsystem
CVE-2024-30087	No	No	Win32k
CVE-2024-30088	No	No	Kernel
CVE-2024-30091	No	No	Win32k
CVE-2024-30093	No	No	Storage
CVE-2024-30094	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30095	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-30096	No	No	Cryptographic Services

CVE	Public	Exploited	Product
CVE-2024-30097	No	No	SAPI
CVE-2024-30099	No	No	Kernel
CVE-2024-35265	No	No	Perception Service
CVE-2024-5493	No	No	Chromium
CVE-2024-5498	No	No	Chromium
CVE-2024-5496	No	No	Chromium
CVE-2024-5499	No	No	Chromium
CVE-2024-5494	No	No	Chromium
CVE-2024-5497	No	No	Chromium
CVE-2024-5495	No	No	Chromium
CVE-2024-30100	No	No	SharePoint Server
CVE-2024-30101	No	No	Office
CVE-2024-30102	No	No	Office
CVE-2024-30103	No	No	Outlook

CVE	Public	Exploited	Product
CVE-2024-30104	No	No	Office
CVE-2024-35255	No	No	Azure Identity Libraries and Authentication Library
CVE-2024-29187	No	No	GitHub
CVE-2024-29060	No	No	Visual Studio
CVE-2024-30066	No	No	Winlogon
CVE-2024-30067	No	No	WinLogon
CVE-2024-30089	No	No	Streaming Service
CVE-2024-30090	No	No	Streaming Service
CVE-2024-35248	No	No	Dynamics 365 Business Central
CVE-2024-35249	No	No	Dynamics 365 Business Central
CVE-2024-35252	No	No	Azure Storage Movement Client Library
CVE-2024-35253	No	No	Azure File Sync
CVE-2024-35254	No	No	Azure Monitor Agent
CVE-2024-35263	No	No	Dynamics 365

CVE	Public	Exploited	Product
CVE-2024-37325	No	No	Azure Science Virtual Machine (DSVM)
CVE-2024-30052	No	No	Visual Studio