Microsoft

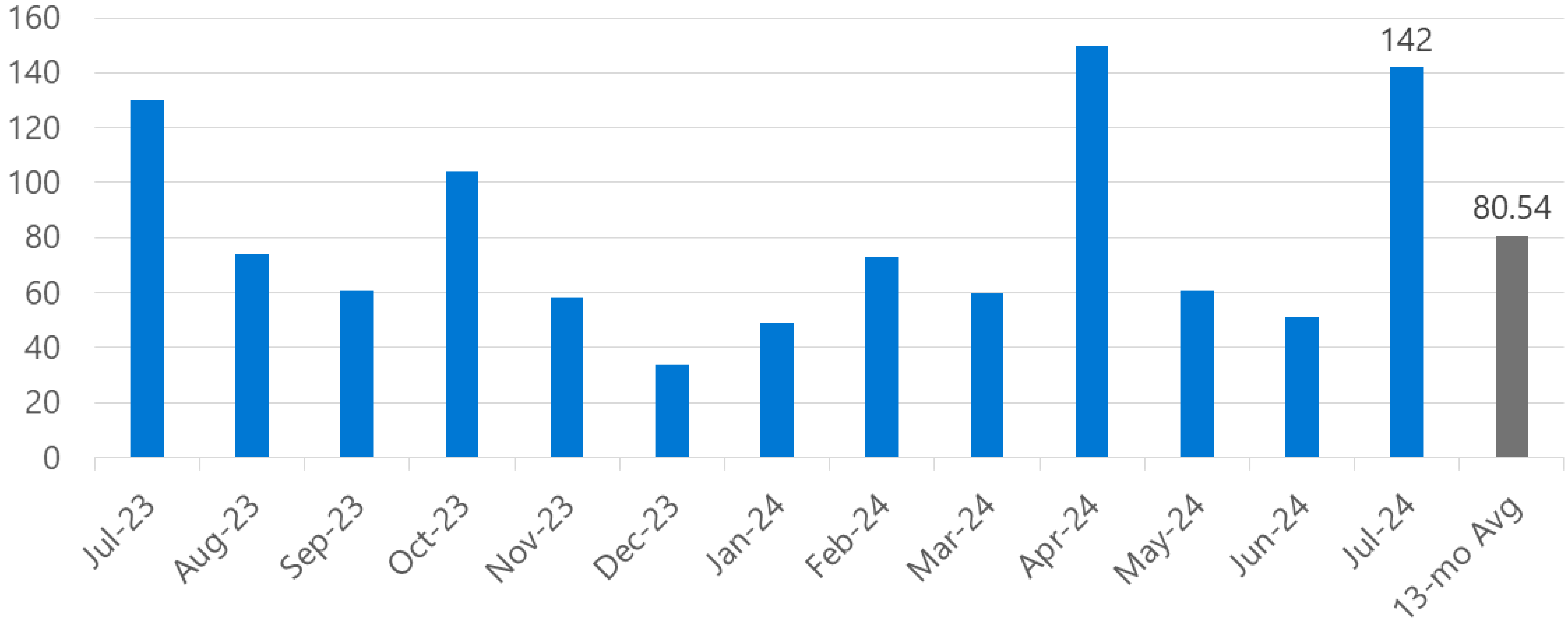
Microsoft Security Release

July 9, 2024

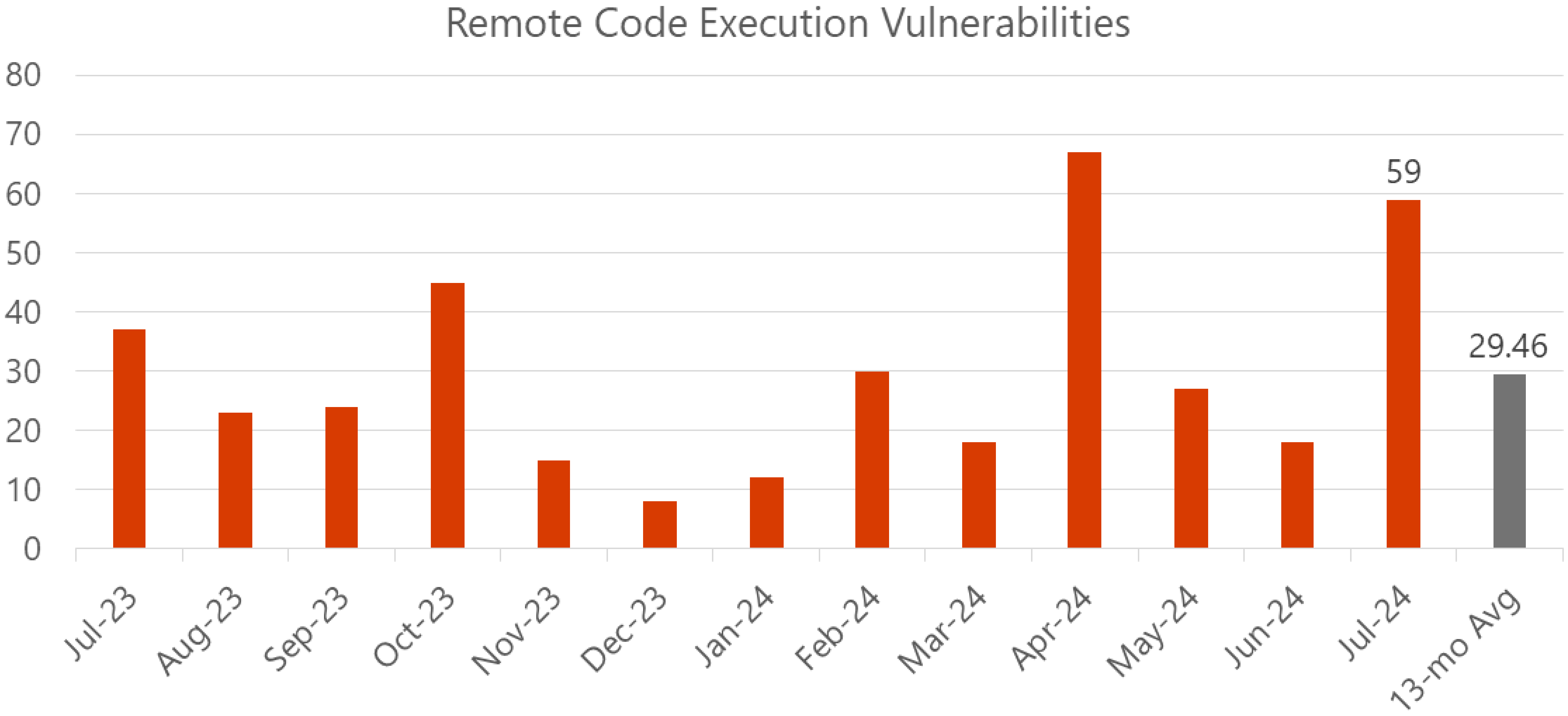
Agenda

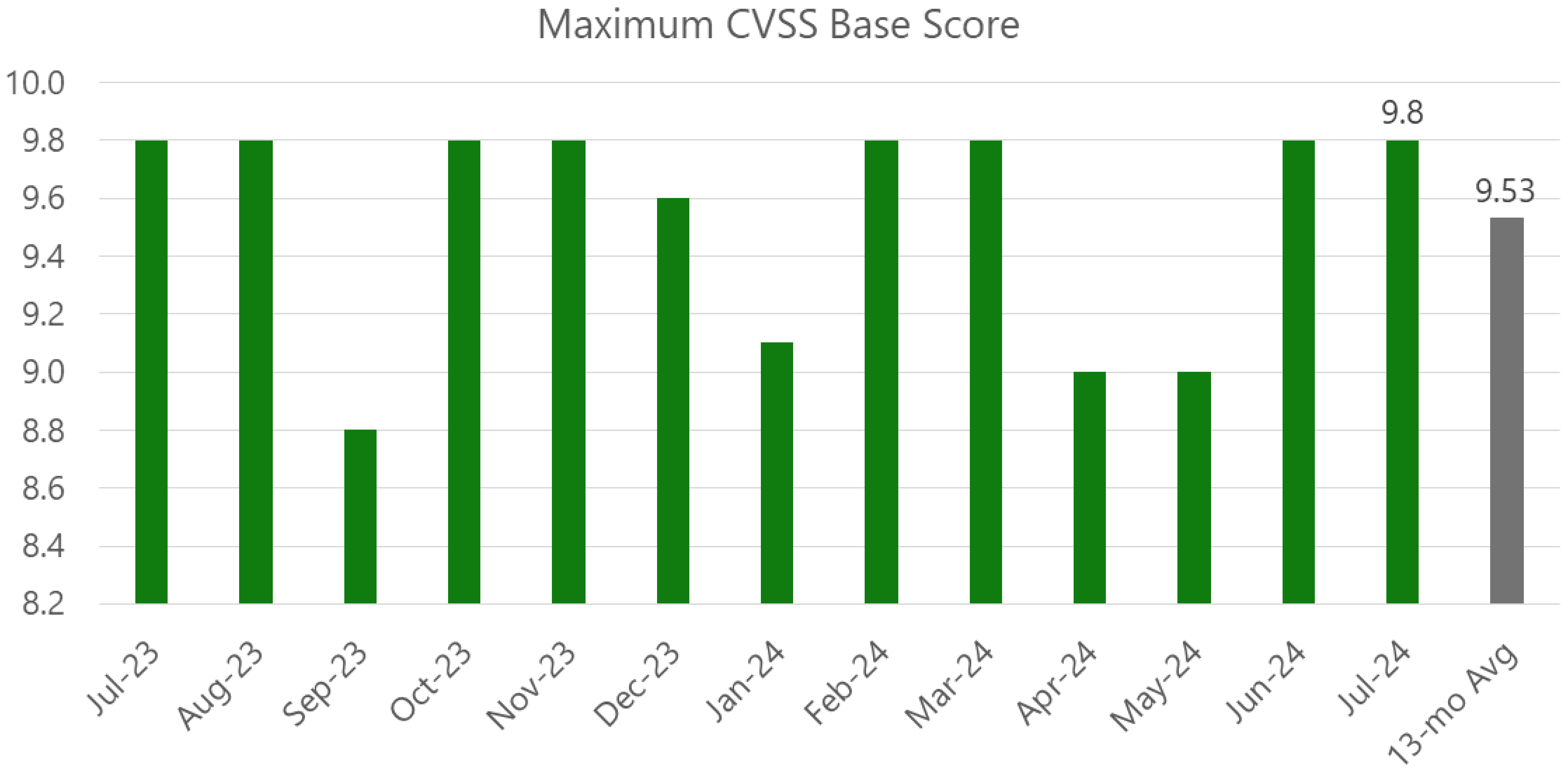
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

Vulnerabilities per month



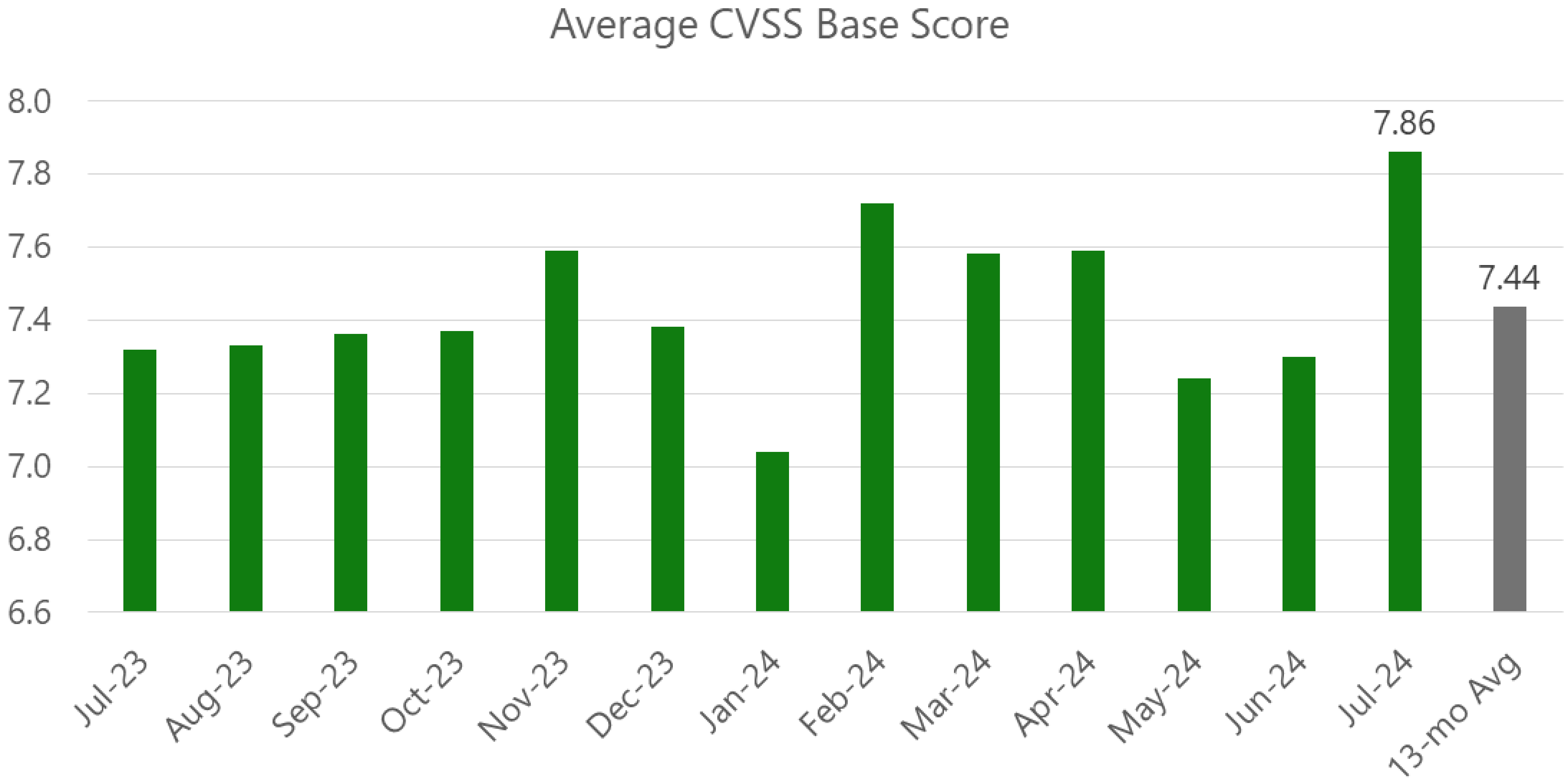
Microsoft


Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
59
29.46
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
13-mo Avg

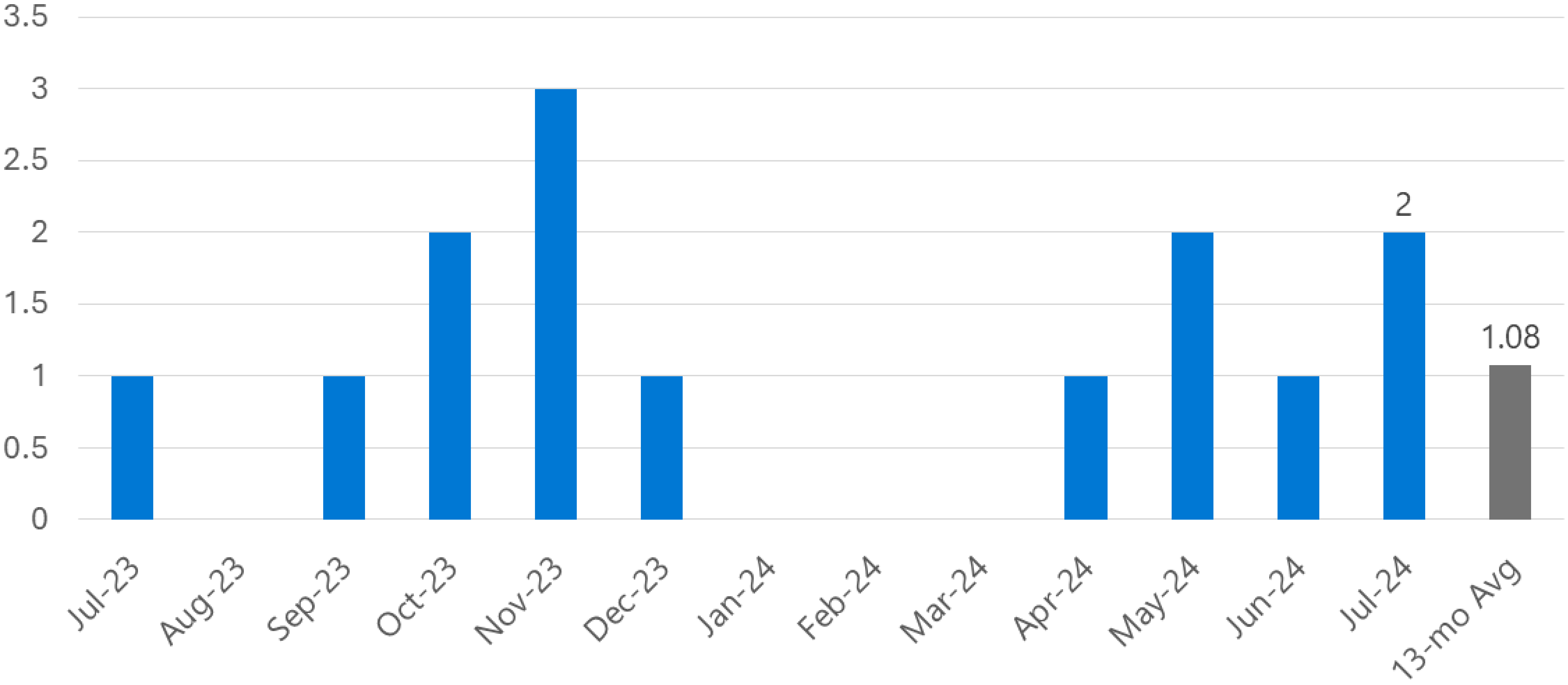


Maximum CVSS Base Score
10.0
9.8
9.6
9.4
9.2
9.0
8.8
8.6
8.4
8.2
9.8
9.53
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
13-mo Avg

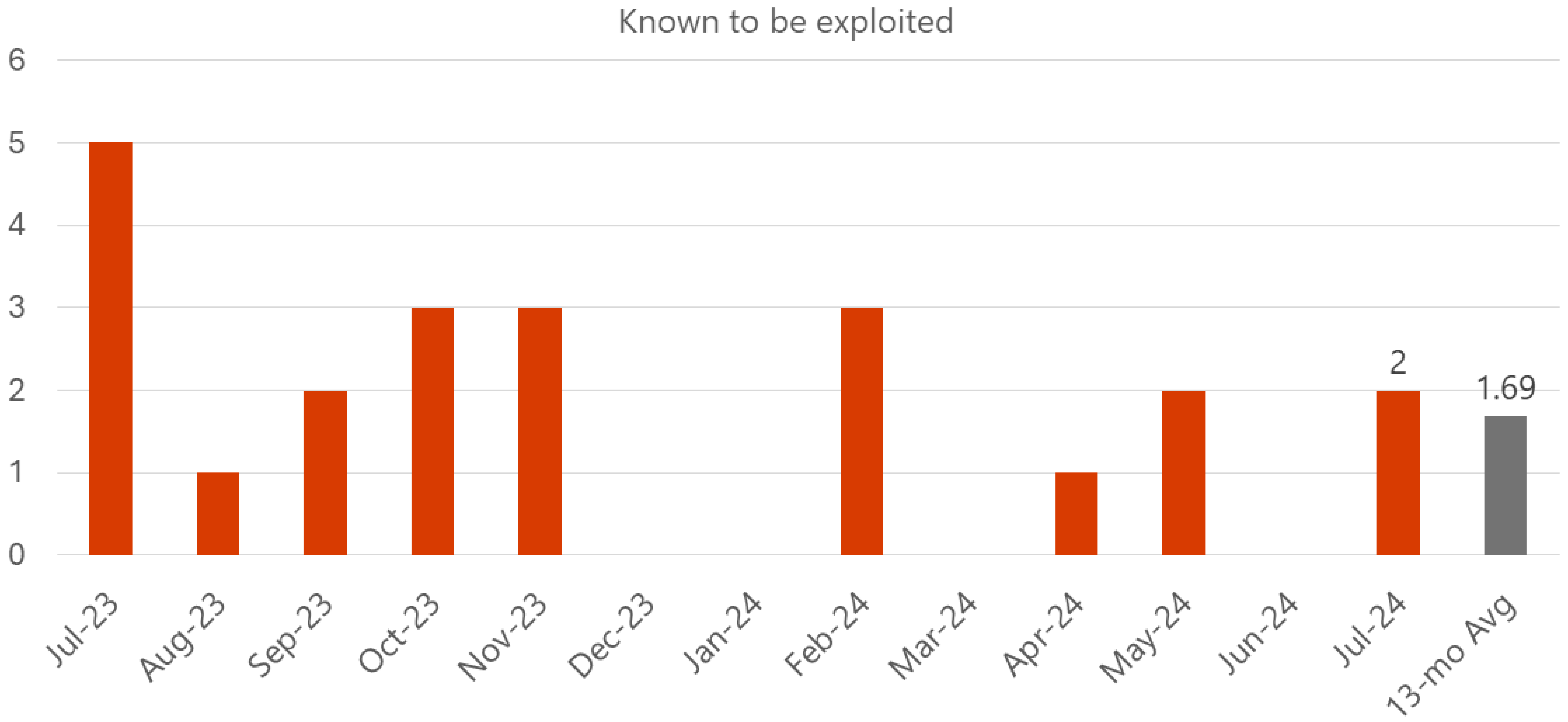
Microsoft


Average CVSS Base Score
8.0
7.8
7.6
7.4
7.2
7.0
6.8
6.6
7.86
7.44
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
13-mo Avg

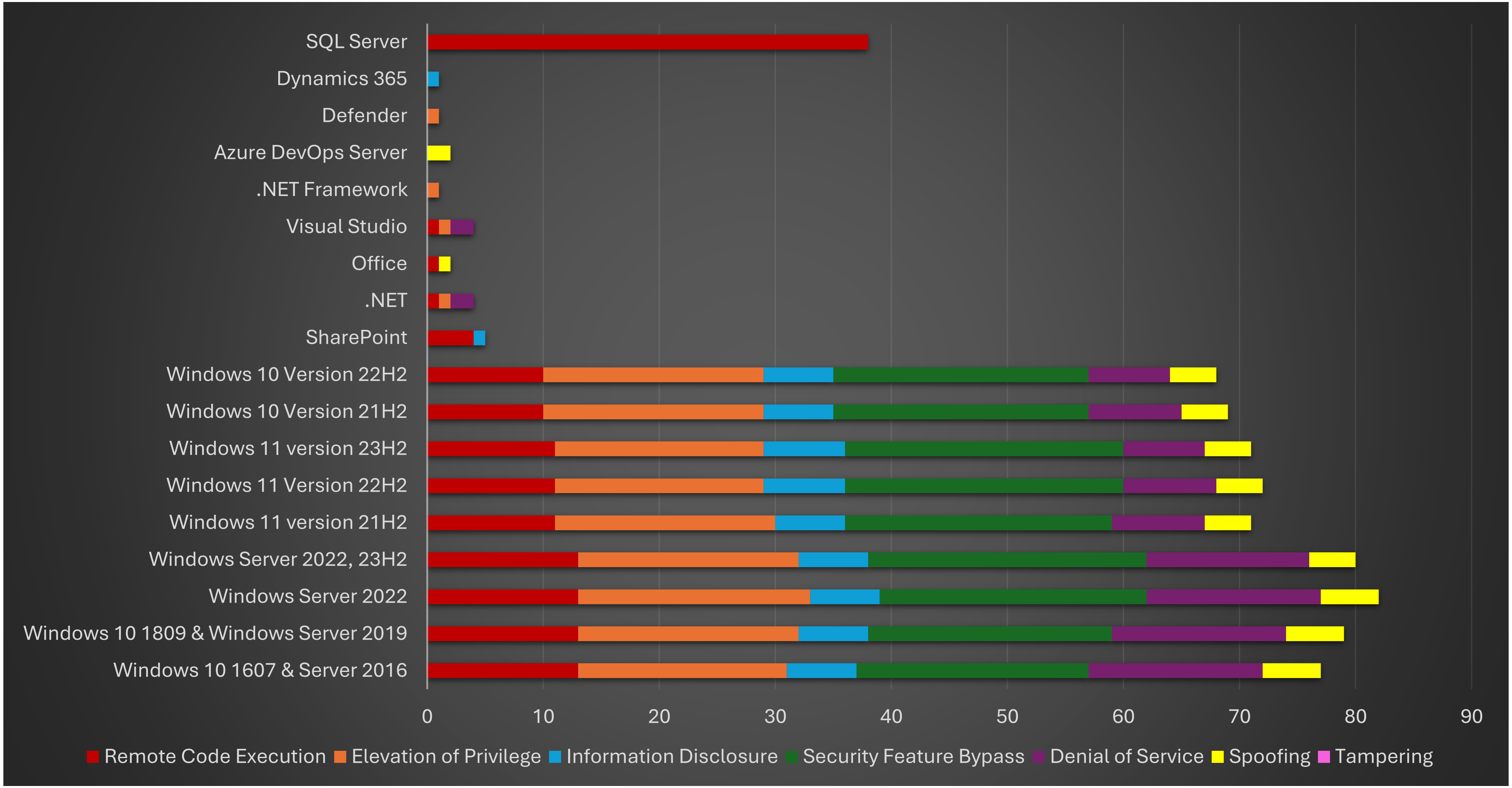
Publicly Disclosed



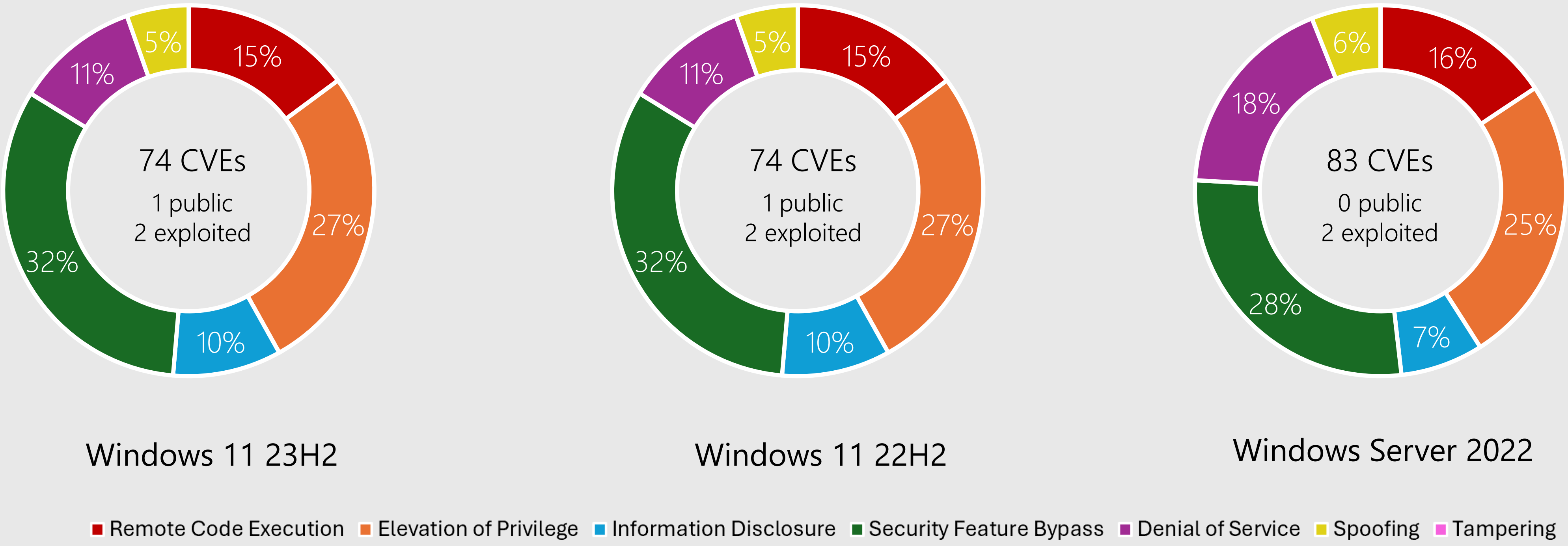
Microsoft


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

Microsoft Security Release Overview – July 2024



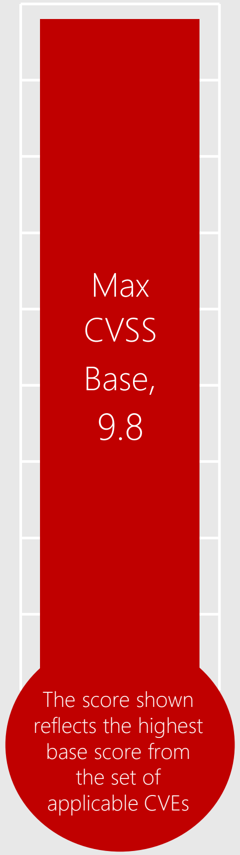
Windows 11, Server 2022



Windows 11 23H2

Windows 11 22H2

Windows Server 2022



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

Affected Components:

See Appendix for details

CVE-2024-38077 Remote Desktop Licensing

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

Disable Remote Desktop Licensing Service if is not required

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server 2019
Server 2016

CVE-2024-38080 Hyper-V

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
Server 2022

CVE-2024-38053 L2 Bridge Network 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-2024-28899 Secure Boot

Impact, Severity, Disclosure

Security Feature Bypass | 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.

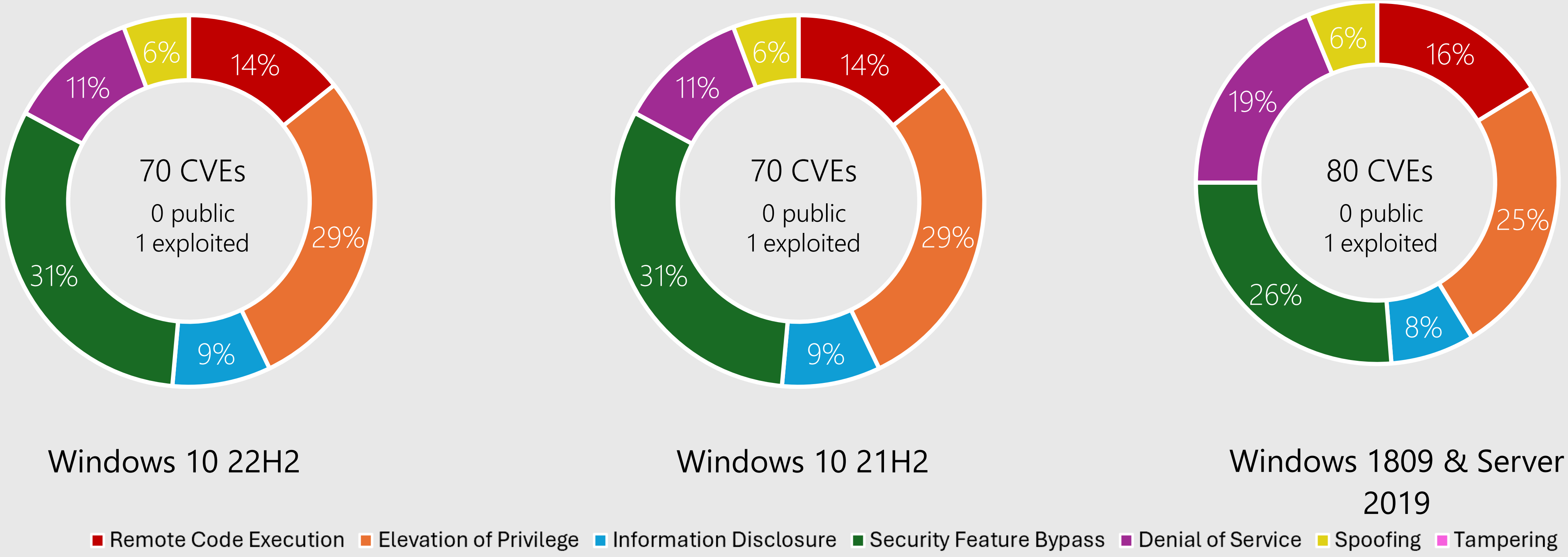
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

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-2024-30013 Windows MultiPoint Services

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-2024-21417 Windows Text Services

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

CVE-2024-38060 Windows Imaging Component

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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38104 Fax 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

To be exploitable by this vulnerability the Windows Fax Service must be installed and configured.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-38112 MSHTML Platform

Impact, Severity, Disclosure

Spoofing | Important | Privately disclosed | Exploitation detected

CVSSScoreMetrics

Base CVSS Score: 7.0 | Attack Vector: Local | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

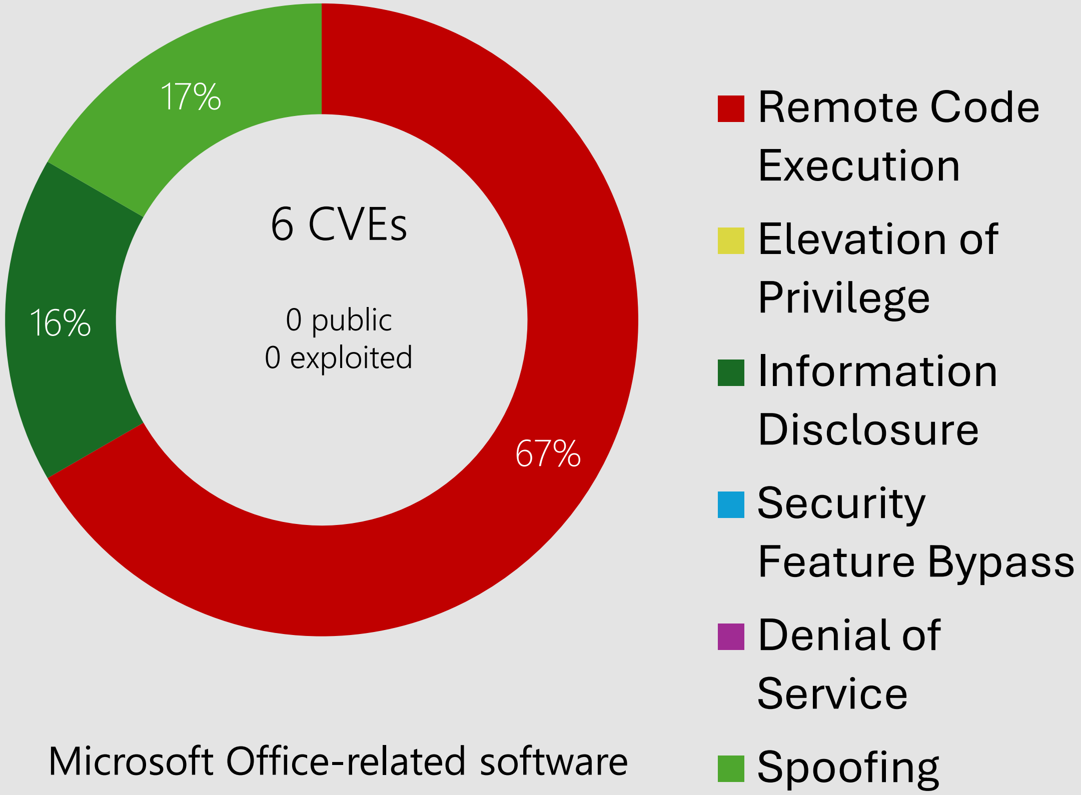
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

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

CVE-2024-38023 SharePoint

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | 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 2019
SharePoint 2016
SharePoint Server Subscription Edition

CVE-2024-38021 Office

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

Office 2016
Office 2019
Office 365 Apps for Enterprise
Office LTSC

Other Products

Dynamics 365

CVE-2024-30061 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Microsoft Dynamics 365 (on-premises) version 9.1

SQL Drivers

SQL Server

37 CVEs | SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability

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

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: Required
Affected Products: SQL Server 2022, SQL Server 2019, SQL Server 2017, SQL Server 2016

CVE List: CVE-2024-20701, CVE-2024-21303, CVE-2024-21308, CVE-2024-21317, CVE-2024-21331, CVE-2024-21332, CVE-2024-21333, CVE-2024-21335, CVE-2024-21373, CVE-2024-21398, CVE-2024-21414, CVE-2024-21415, CVE-2024-21425, CVE-2024-21428, CVE-2024-21449, CVE-2024-28928, CVE-2024-35256, CVE-2024-35271, CVE-2024-35272, CVE-2024-37318, CVE-2024-37319, CVE-2024-37320, CVE-2024-37321, CVE-2024-37322, CVE-2024-37323, CVE-2024-37324, CVE-2024-37326, CVE-2024-37327, CVE-2024-37328, CVE-2024-37329, CVE-2024-37330, CVE-2024-37331, CVE-2024-37332,CVE-2024-37333, CVE-2024-37336,CVE-2024-38087,CVE-2024-38088

CVE-2024-37334 | OLE DB Driver for SQL Server Remote Code Execution Vulnerability

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

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: Required
Affected Products: SQL Server 2022, SQL Server 2019, OLE DB Driver 19 for SQL Server, OLE DB Driver 18 for SQL Server

Developer Tools

Microsoft .NET, .NET Framework, Visual Studio

CVE-2024-35264 | .NET and Visual Studio Remote Code Execution Vulnerability

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

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

Affected Products: .NET 8.0, Visual Studio 2022

CVE-2024-38081 | .NET and Visual Studio Elevation of Privilege

Base CVSS: 7.3 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: Yes

Affected Products: .NET 8.0, .NET Framework, Visual Studio 2022

Developer Tools

Microsoft .NET, .NET Framework, Visual Studio

CVE-2024-30105 | .NET 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 8.0, Visual Studio 2022

CVE-2024-38095 | .NET 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 8.0, Visual Studio 2022

Developer Tools

Azure DevOps

CVE-2024-35266 | Azure DevOps Spoofing Vulnerability

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

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

Affected Products: Azure DevOps Server 2020.1.2

CVE-2024-35267 | Azure DevOps Spoofing Vulnerability

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

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

Affected Products: Azure DevOps Server 2020.1.2

Other Products

Azure, Defender

CVE-2024-35261 Azure Network Watcher

CVE-2024-38092 Azure CycleCloud

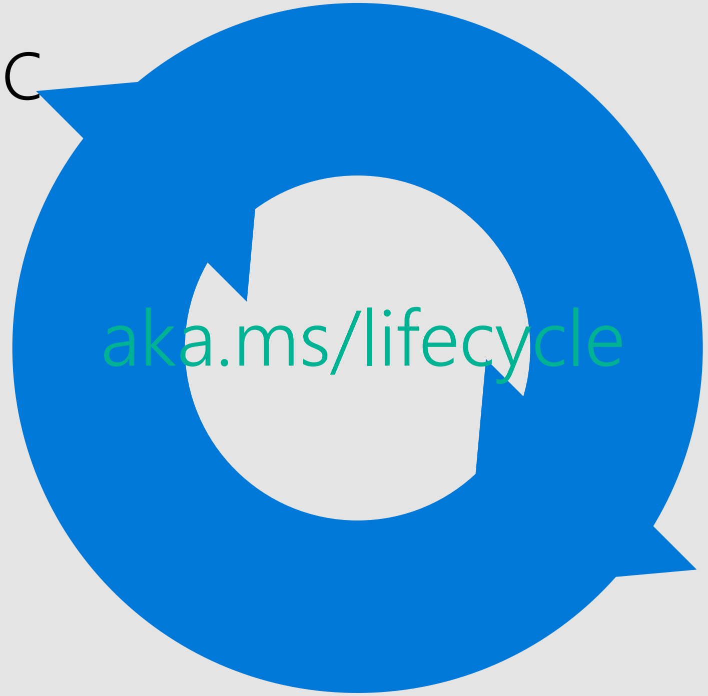
CVE-2024-38089 Microsoft Defender for IoT

CVE-2024-38086 Azure Kinect SDK

Product Lifecycle Update

Products reaching end of support

Microsoft SQL Server 2012, ESU Year 2
SQL Server 2014
Visual Studio 2022 , v17.4 LTSC



aka.ms/lifecycle

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

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2024-21417	No	No	Text Services Framework
CVE-2024-28899	No	No	Secure Boot
CVE-2024-30081	No	No	NTLM
CVE-2024-30098	No	No	Cryptographic Services
CVE-2024-35270	No	No	iSCSI Service
CVE-2024-37969	No	No	Secure Boot
CVE-2024-37970	No	No	Secure Boot
CVE-2024-37974	No	No	Secure Boot
CVE-2024-37981	No	No	Secure Boot
CVE-2024-37986	No	No	Secure Boot
CVE-2024-37987	No	No	Secure Boot
CVE-2024-38013	No	No	Server Backup
CVE-2024-38015	No	No	Remote Desktop Gateway (RD Gateway)
CVE-2024-38022	No	No	Image Acquisition
CVE-2024-38112	No	Yes	MSHTML Platform

CVE	Public	Exploited	Product
CVE-2024-38025	No	No	Performance Data Helper Library
CVE-2024-38034	No	No	Filtering Platform
CVE-2024-38041	No	No	Kernel
CVE-2024-38043	No	No	PowerShell
CVE-2024-38051	No	No	Graphics Component
CVE-2024-38055	No	No	Codecs Library
CVE-2024-38056	No	No	Codecs Library
CVE-2024-38059	No	No	Win32k
CVE-2024-38060	No	No	Codecs Library
CVE-2024-38062	No	No	Kernel-Mode Driver
CVE-2024-38064	No	No	TCP/IP
CVE-2024-38071	No	No	Remote Desktop Licensing Service
CVE-2024-38072	No	No	Remote Desktop Licensing Service
CVE-2024-38077	No	No	Remote Desktop Licensing Service

CVE	Public	Exploited	Product
CVE-2024-38080	No	Yes	Hyper-V
CVE-2024-38085	No	No	Graphics Component
CVE-2024-38100	No	No	File Explorer
CVE-2024-38102	No	No	Layer-2 Bridge Network Driver
CVE-2024-38104	No	No	Fax Service
CVE-2024-26184	No	No	Secure Boot
CVE-2024-30013	No	No	MultiPoint Services
CVE-2024-30071	No	No	Remote Access Connection Manager
CVE-2024-30079	No	No	Remote Access Connection Manager
CVE-2024-37971	No	No	Secure Boot
CVE-2024-37972	No	No	Secure Boot
CVE-2024-37973	No	No	Secure Boot
CVE-2024-37975	No	No	Secure Boot
CVE-2024-37977	No	No	Secure Boot

CVE	Public	Exploited	Product
CVE-2024-37978	No	No	Secure Boot
CVE-2024-37984	No	No	Secure Boot
CVE-2024-37988	No	No	Secure Boot
CVE-2024-37989	No	No	Secure Boot
CVE-2024-38010	No	No	Secure Boot
CVE-2024-38011	No	No	Secure Boot
CVE-2024-38017	No	No	Message Queuing
CVE-2024-38019	No	No	Performance Data Helper Library
CVE-2024-38027	No	No	Line Printer Daemon Service
CVE-2024-38028	No	No	Performance Data Helper Library
CVE-2024-38030	No	No	Themes
CVE-2024-38031	No	No	Online Certificate Status Protocol (OCSP) Server
CVE-2024-38033	No	No	PowerShell
CVE-2024-38044	No	No	DHCP Server Service

CVE	Public	Exploited	Product
CVE-2024-38047	No	No	PowerShell
CVE-2024-38048	No	No	Network Driver Interface Specification (NDIS)
CVE-2024-38049	No	No	Distributed Transaction Coordinator
CVE-2024-38050	No	No	Workstation Service
CVE-2024-38053	No	No	Layer-2 Bridge Network Driver
CVE-2024-38058	No	No	BitLocker
CVE-2024-38065	No	No	Secure Boot
CVE-2024-38066	No	No	Win32k
CVE-2024-38067	No	No	Online Certificate Status Protocol (OCSP) Server
CVE-2024-38068	No	No	Online Certificate Status Protocol (OCSP) Server
CVE-2024-38069	No	No	Enroll Engine
CVE-2024-38070	No	No	LockDown Policy (WLDP)
CVE-2024-38073	No	No	Remote Desktop Licensing Service
CVE-2024-38074	No	No	Remote Desktop Licensing Service

CVE	Public	Exploited	Product
CVE-2024-38076	No	No	Remote Desktop Licensing Service
CVE-2024-38079	No	No	Graphics Component
CVE-2024-38099	No	No	Remote Desktop Licensing Service
CVE-2024-38101	No	No	Layer-2 Bridge Network Driver
CVE-2024-38105	No	No	Layer-2 Bridge Network Driver
CVE-2024-38023	No	No	SharePoint Server
CVE-2024-38024	No	No	SharePoint Server
CVE-2024-32987	No	No	SharePoint Server
CVE-2024-38020	No	No	Outlook
CVE-2024-38021	No	No	Office
CVE-2024-38094	No	No	SharePoint
CVE-2024-30061	No	No	Dynamics 365 (On-Premises)
CVE-2024-35264	Yes	No	.NET and Visual Studio
CVE-2024-38088	No	No	SQL Server Native Client OLE DB Provider

CVE	Public	Exploited	Product
CVE-2024-38087	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21332	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21333	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21335	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21373	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21398	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21414	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21415	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21428	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37318	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37332	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37331	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37985	Yes	No	Arm: CVE-2024-37985 Systematic Identification and Characterization of Proprietary Prefetchers

CVE	Public	Exploited	Product
CVE-2024-38054	No	No	Kernel Streaming WOW Thunk Service Driver
CVE-2024-38061	No	No	DCOM Remote Cross-Session Activation
CVE-2024-38086	No	No	Azure Kinect SDK
CVE-2024-38091	No	No	WS-Discovery
CVE-2024-3596	No	No	CERT/CC: CVE-2024-3596 RADIUS Protocol
CVE-2024-30105	No	No	.NET Core and Visual Studio
CVE-2024-35261	No	No	Azure Network Watcher VM Extension
CVE-2024-35266	No	No	Azure DevOps Server
CVE-2024-35267	No	No	Azure DevOps Server
CVE-2024-35271	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-35272	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-20701	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21303	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21308	No	No	SQL Server Native Client OLE DB Provider

CVE	Public	Exploited	Product
CVE-2024-21317	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21331	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21425	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37319	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37320	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37321	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37322	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37323	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37324	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-21449	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37326	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37327	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37328	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37329	No	No	SQL Server Native Client OLE DB Provider

CVE	Public	Exploited	Product
CVE-2024-37330	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37334	No	No	OLE DB Driver for SQL Server
CVE-2024-37333	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-37336	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-28928	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-35256	No	No	SQL Server Native Client OLE DB Provider
CVE-2024-38032	No	No	Xbox
CVE-2024-38052	No	No	Kernel Streaming WOW Thunk Service Driver
CVE-2024-38057	No	No	Kernel Streaming WOW Thunk Service Driver
CVE-2024-38078	No	No	Xbox Wireless Adapter
CVE-2024-38081	No	No	.NET, .NET Framework, and Visual Studio
CVE-2024-38089	No	No	Defender for IoT
CVE-2024-38092	No	No	Azure CycleCloud
CVE-2024-38095	No	No	.NET and Visual Studio