Microsoft

Microsoft Security Release

April 9, 2024

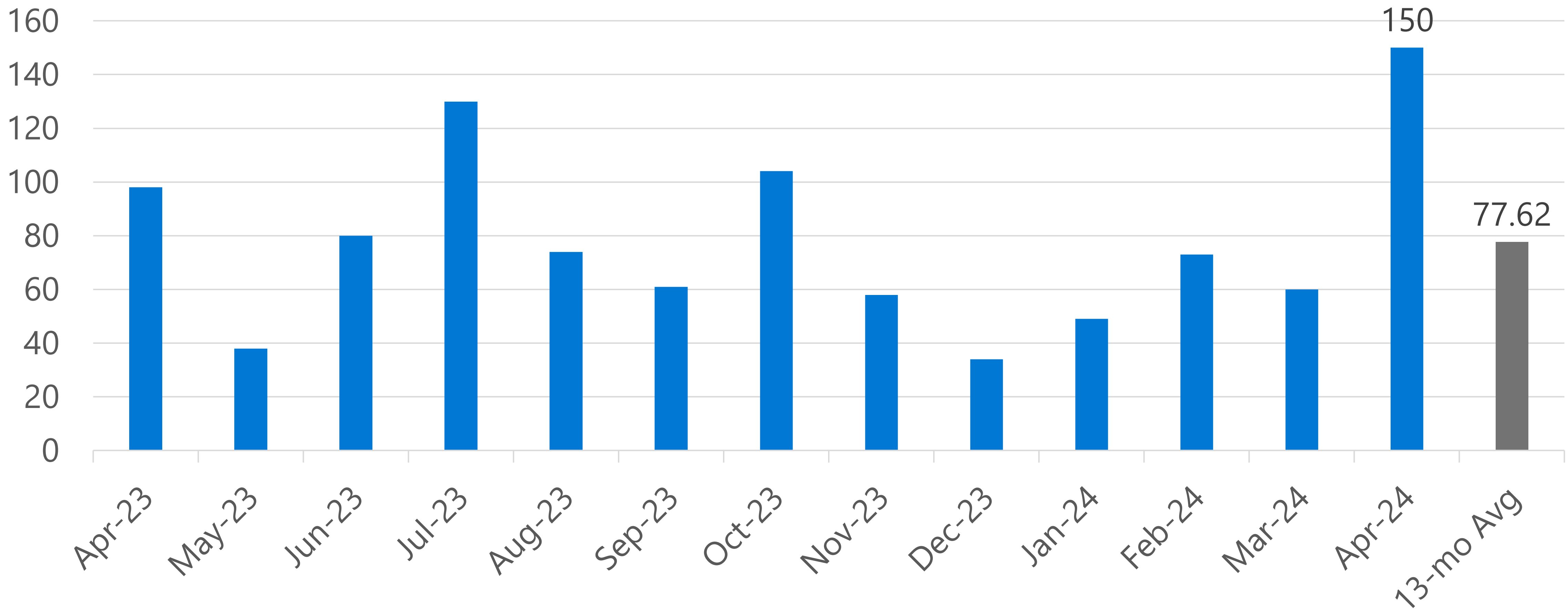
The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Agenda

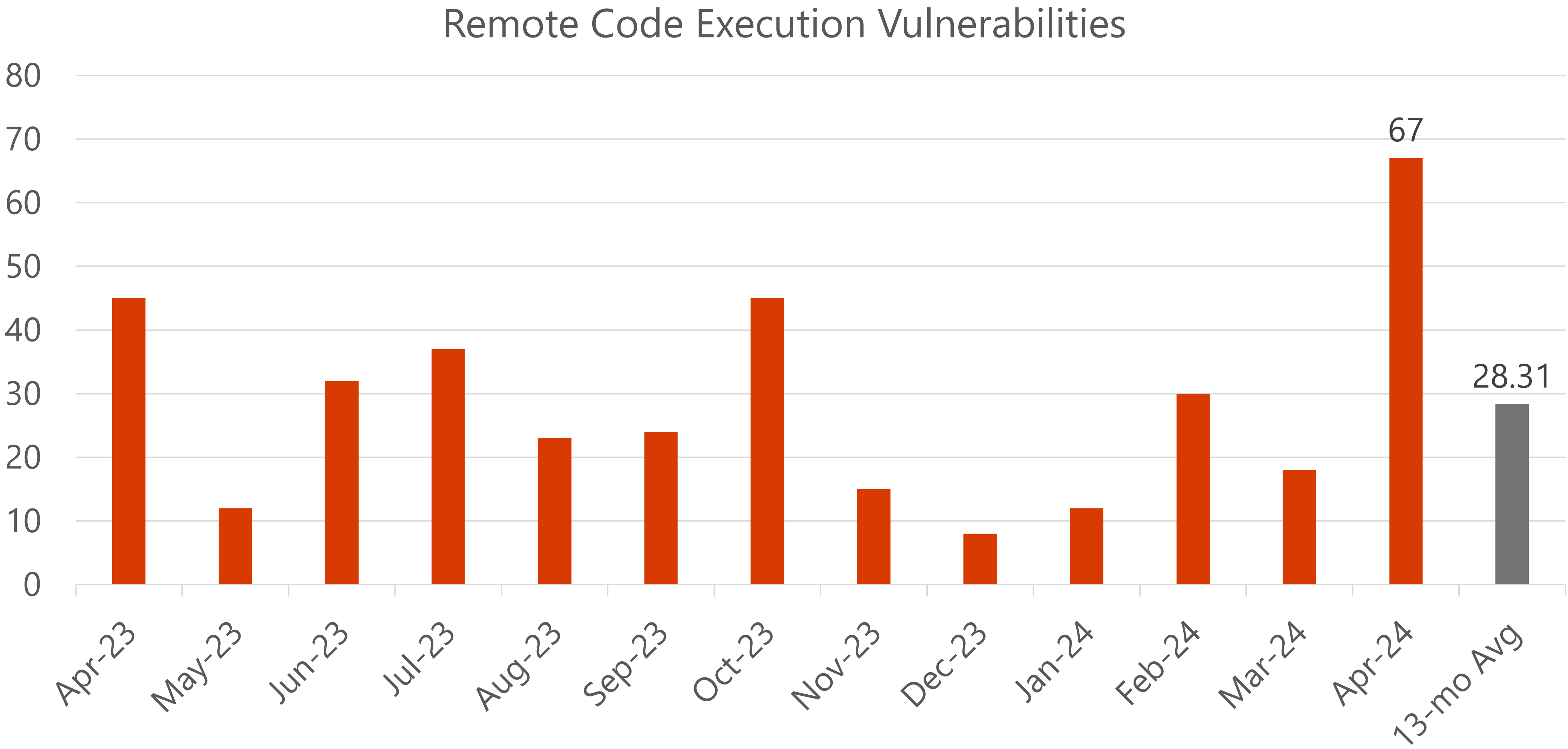
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

Microsoft

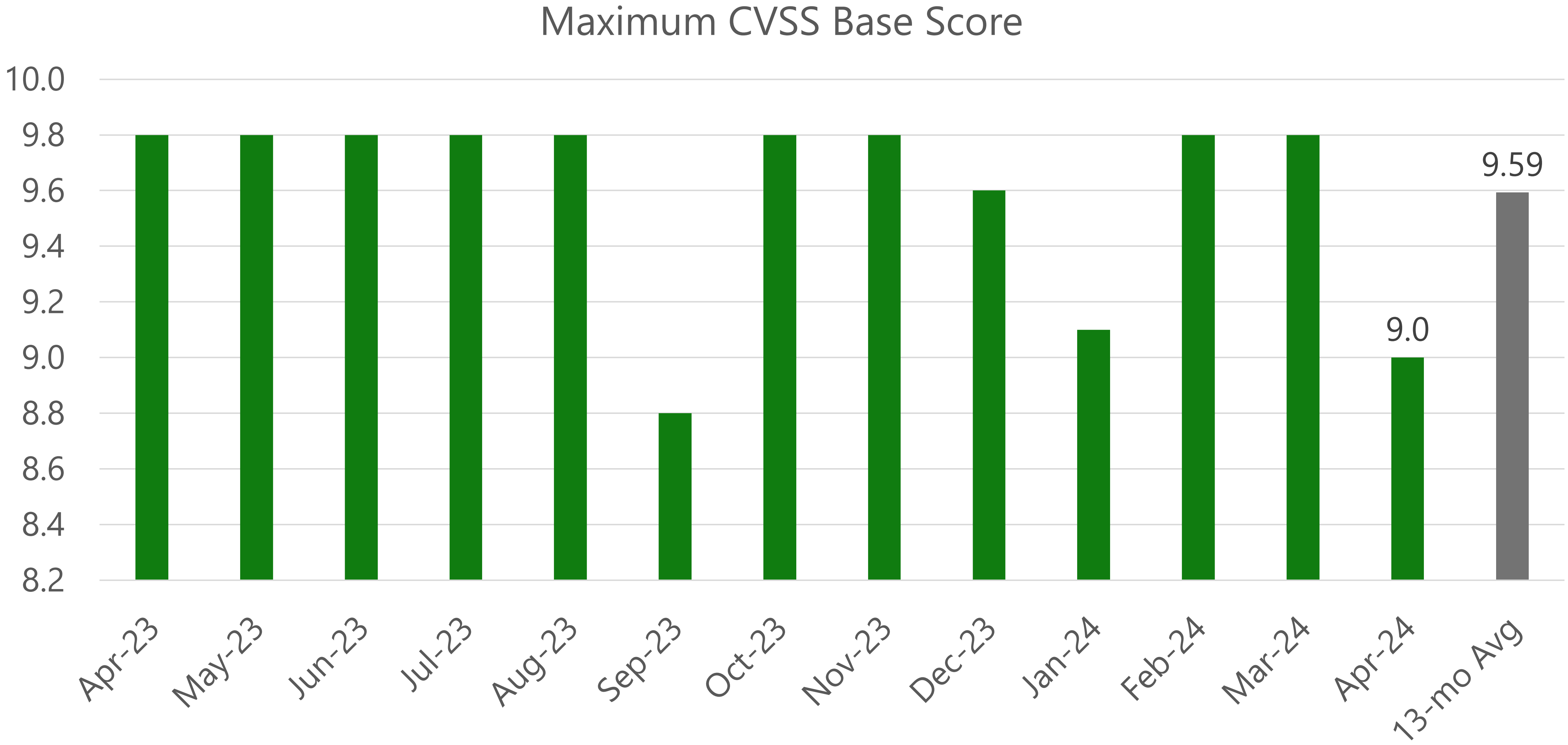
Vulnerabilities per month



Microsoft


Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
67
28.31
Apr-23
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
13-mo Avg

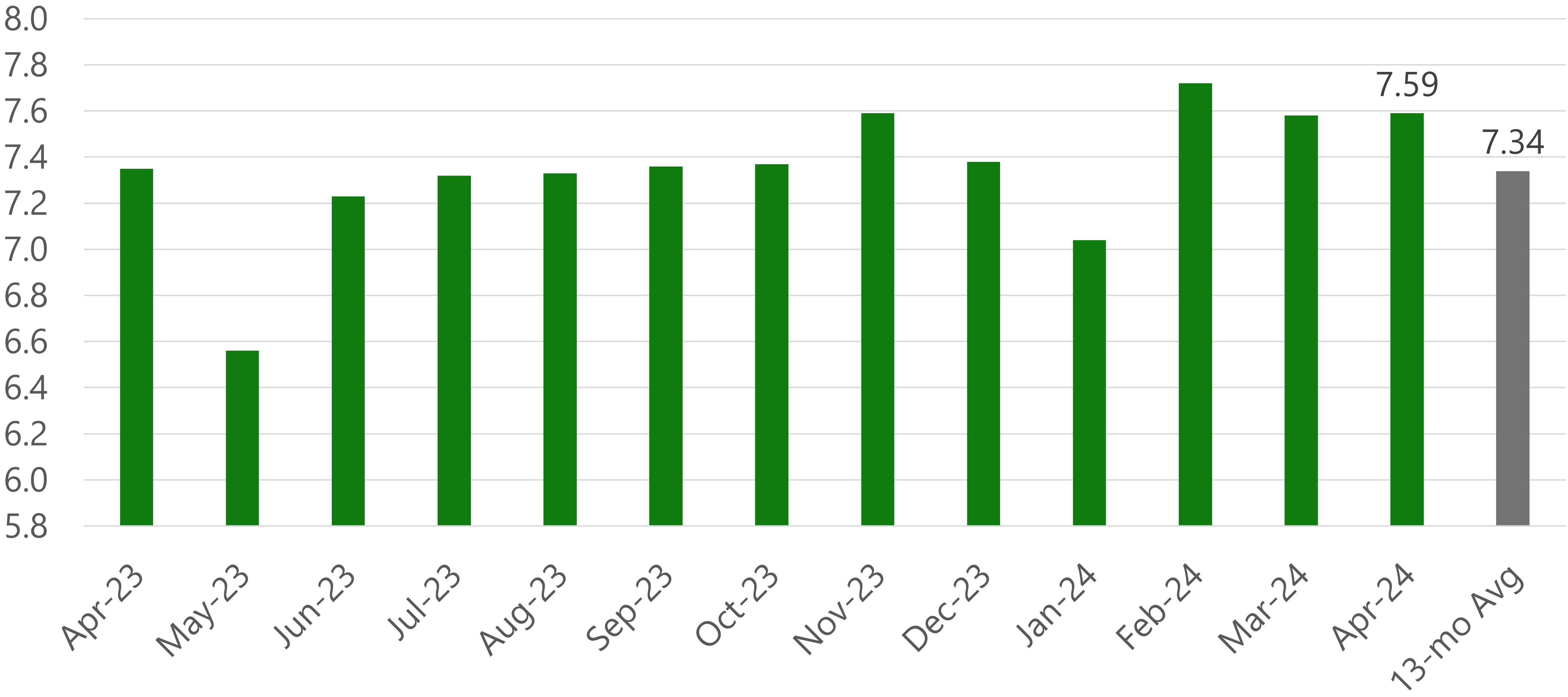
Microsoft

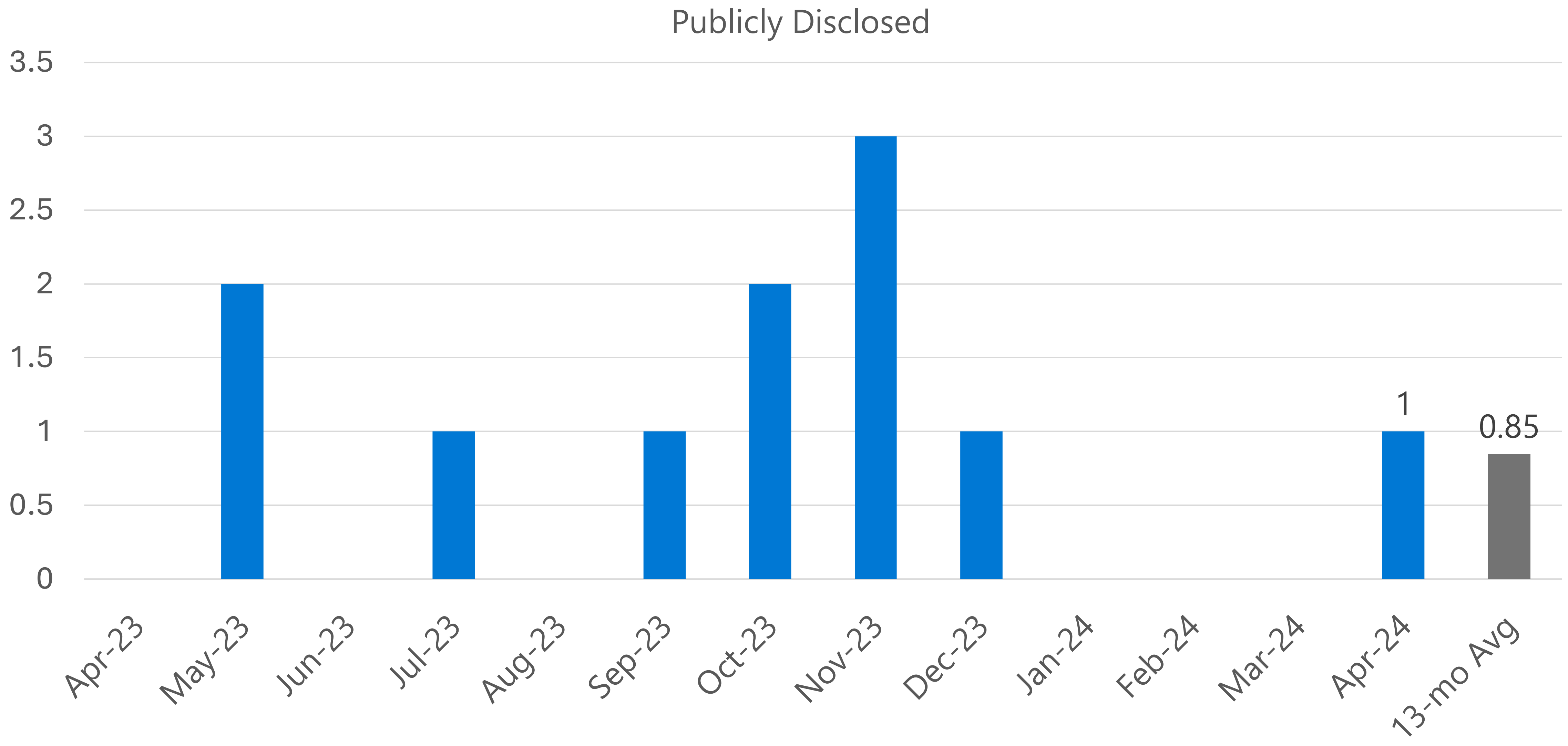


Maximum CVSS Base Score
10.0
9.8
9.6
9.4
9.2
9.0
8.8
8.6
8.4
8.2
9.0
9.59
Apr-23
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
13-mo Avg

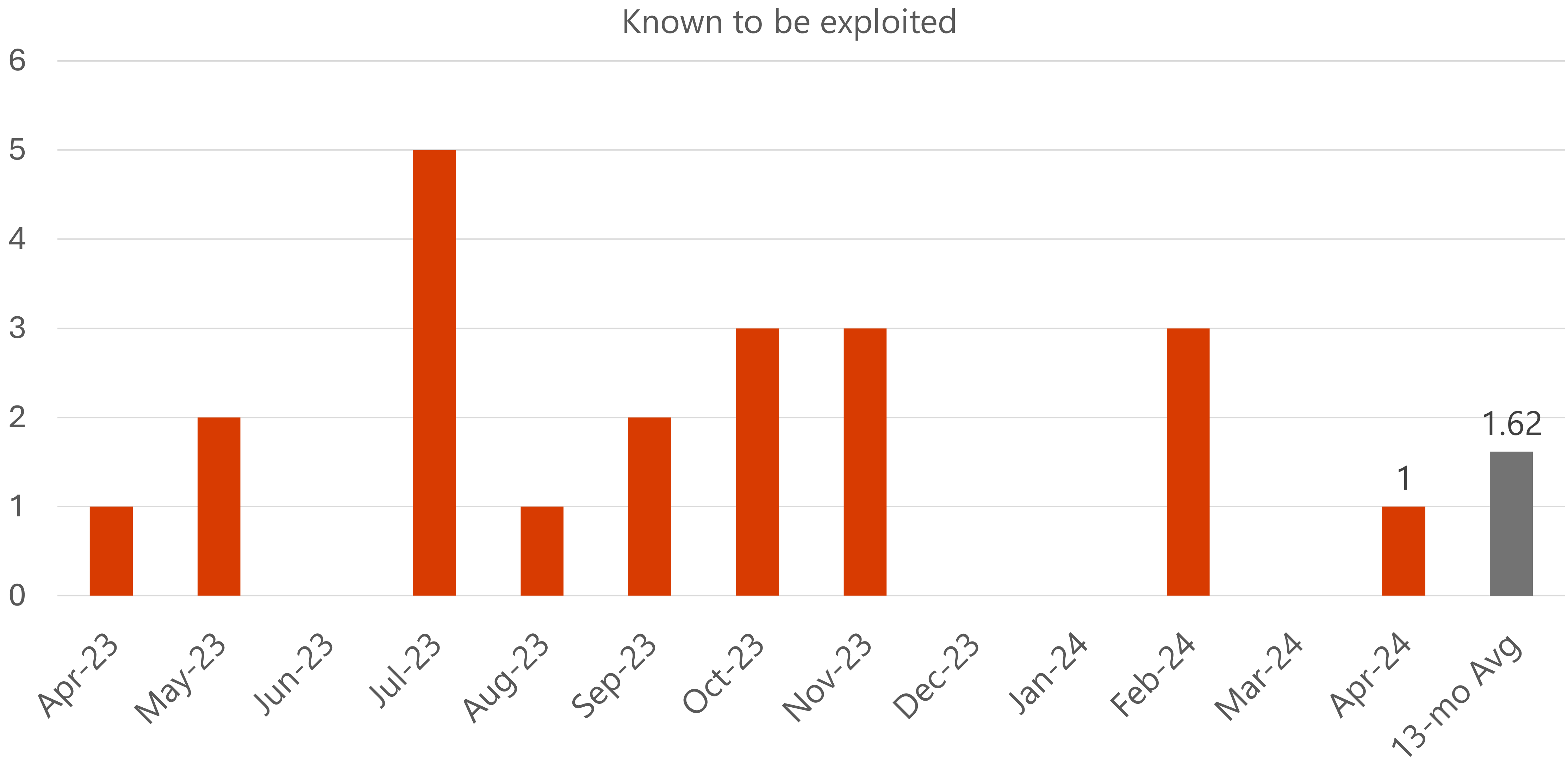
Microsoft

Average CVSS Base Score



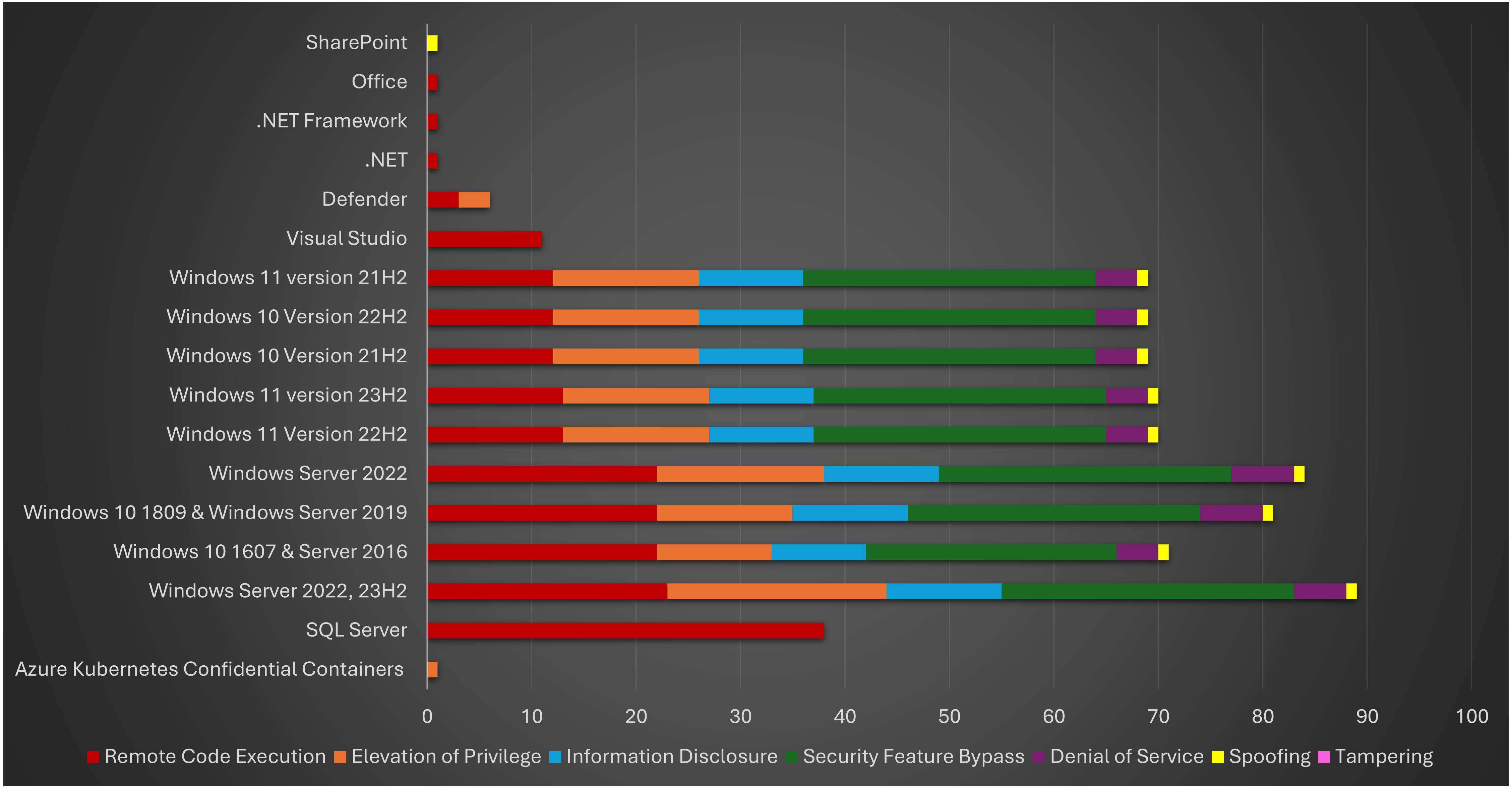

Publicly Disclosed
3.5
3
2.5
2
1.5
1
0.5
0
1
0.85
Apr-23
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
13-mo Avg

Microsoft

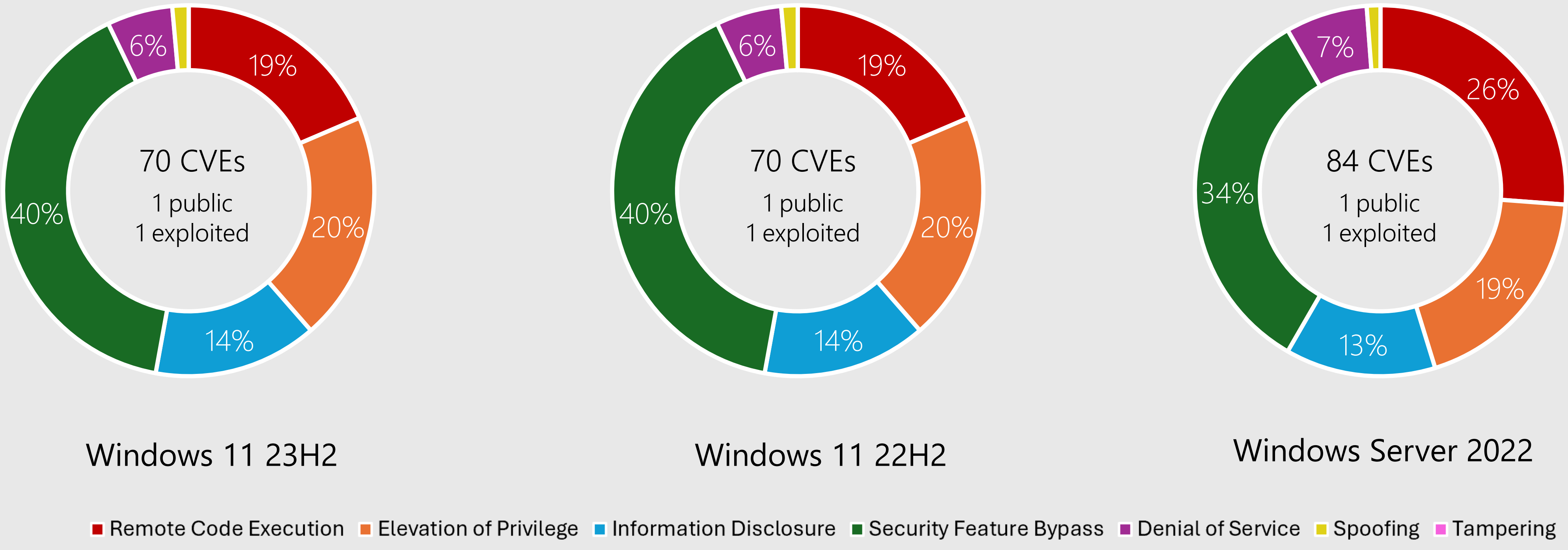


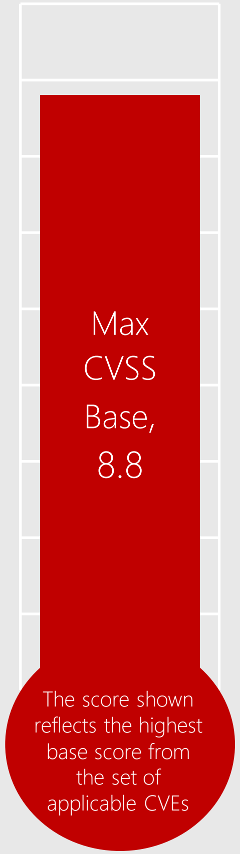
Known to be exploited
6
5
4
3
2
1
0
1
1.62
Apr-23
May-23
Jun-23
Jul-23
Aug-23
Sep-23
Oct-23
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
13-mo Avg

Microsoft Security Release Overview – April 2024



Windows 11, Server 2022





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

Affected Components:

See Appendix for details

CVE-2024-26234 Proxy Driver

Impact, Severity, Disclosure

Spoofing | Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 6.7 | Attack Vector: Local | 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

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-29988 SmartScreen

Impact, Severity, Disclosure

Security Feature Bypass | 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

CVE-2024-26200 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-2024-20678 RPC Runtime

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-2024-26214 WDAC ODBC 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.

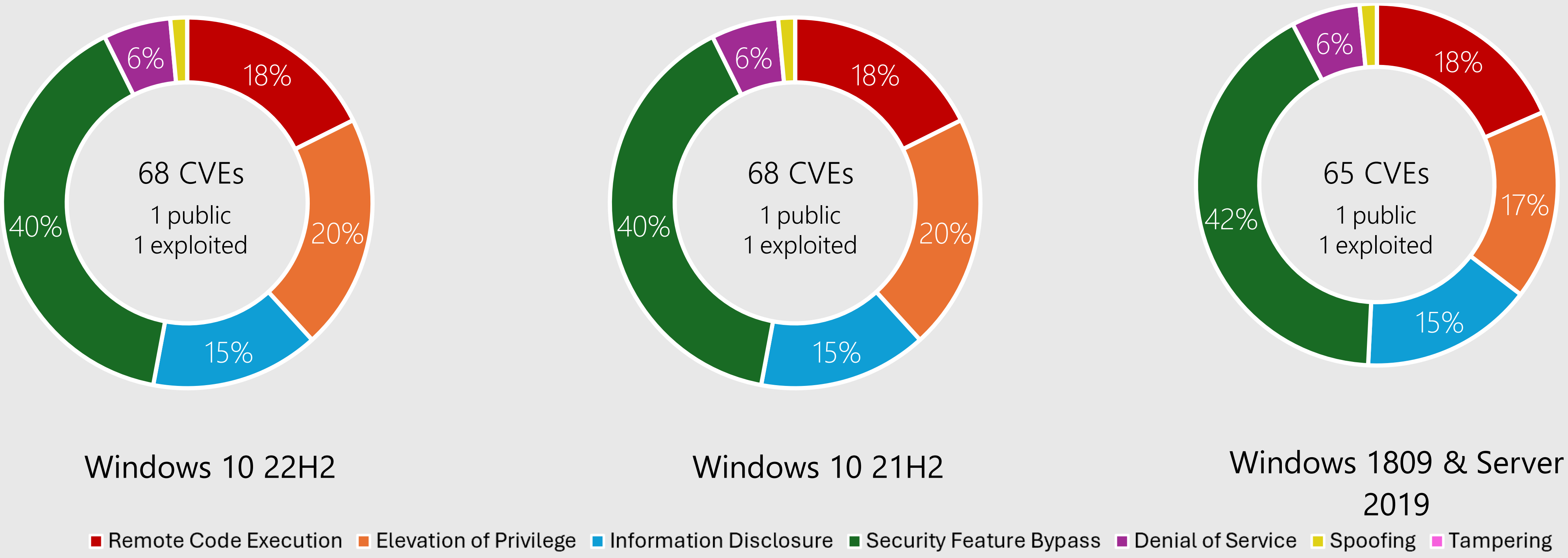
Workarounds

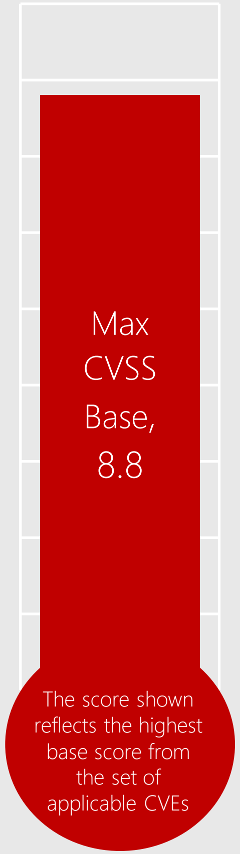
Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Windows 10





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

Affected Components:

See Appendix for details

CVE-2024-29050 Cryptographic Services

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.4 | Attack Vector: Local | 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-2024-26180 Secure Boot

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.0 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Additional steps are required at this time to mitigate this vulnerability. Please refer to How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-29056 Windows Authentication

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 4.3 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

More Information

The updates released on or after April 9, 2024, will NOT fully address the security issues in this vulnerability. For more information about how to manage PAC validation changes related to this CVE and the steps you need to take to be fully protected, see How to manage PAC Validation changes related to CVE-2024-26248 and CVE-2024-29056

Affected Software

Server 2022
Server 2019
Server 2016

CVE-2024-2201 Intel Branch History Injection

Impact, Severity, Disclosure

Information Disclosure | Important | Privately Disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 4.7 | Attack Vector: Local | Attack Complexity: High | Privileges Required: Low | User Interaction: None

Mitigations

Mitigation is disabled by default. See KB4072698 for steps to take to enable full protection.

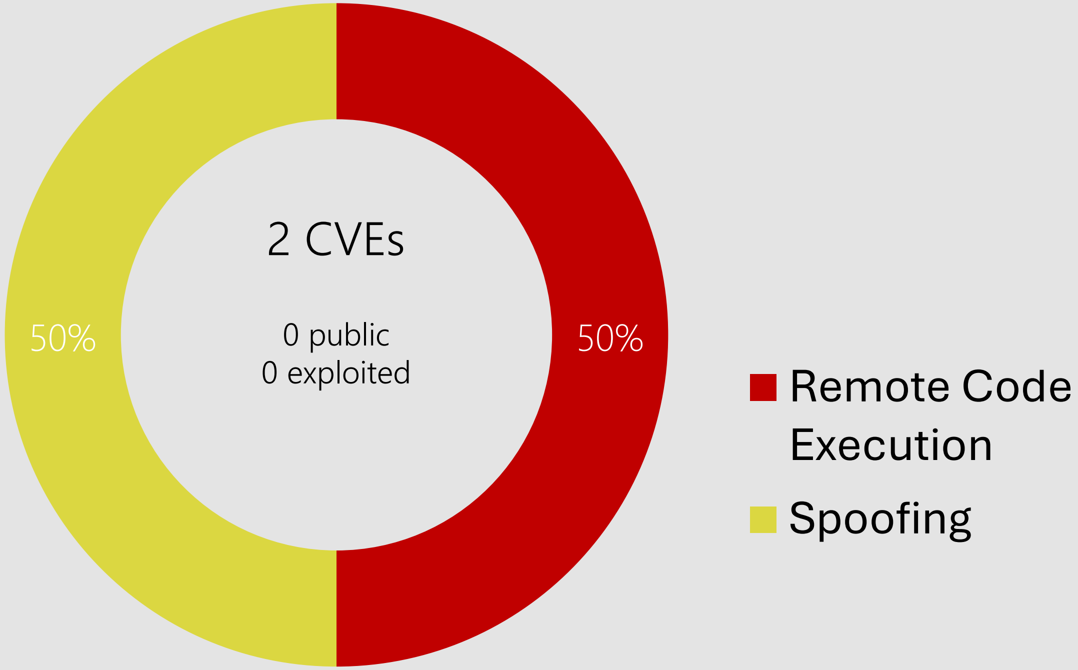
Workarounds

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:

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

CVE-2024-26257 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 365 Apps for Enterprise
Office LTSC for Mac 2021

CVE-2024-26251 SharePoint

Impact, Severity, Disclosure

Spoofing | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 6.8 | Attack Vector: Network | 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

SharePoint 2019
SharePoint 2016
SharePoint Server Subscription Edition

SQL Drivers

SQL Server, ODBC Driver, OLE DB Driver, Visual Studio

13 CVEs | ODBC 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, ODBC Driver 17 for SQL Server on Linux, ODBC Driver 17 for SQL Server on MacOS, ODBC Driver 17 for SQL Server on Windows, ODBC Driver 18 for SQL Server on Linux, ODBC Driver 18 for SQL Server on MacOS, ODBC Driver 18 for SQL Server on Windows, Visual Studio 2022

CVE List: CVE-2024-28929, CVE-2024-28930, CVE-2024-28931, CVE-2024-28932, CVE-2024-28933, CVE-2024-28934, CVE-2024-28935, CVE-2024-28936, CVE-2024-28937, CVE-2024-28938, CVE-2024-28941, CVE-2024-28943, CVE-2024-29043

---

24 CVEs | 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

CVE List: CVE-2024-28906 ,CVE-2024-28908, CVE-2024-28909, CVE-2024-28910,CVE-2024-28911, CVE-2024-28912, CVE-2024-28913, CVE-2024-28914, CVE-2024-28915, CVE-2024-28926, CVE-2024-28927, CVE-2024-28939, CVE-2024-28940, CVE-2024-28942, CVE-2024-28944, CVE-2024-28945, CVE-2024-29044, CVE-2024-29045, CVE-2024-29046, CVE-2024-29047, CVE-2024-29048, CVE-2024-29982, CVE-2024-29983, CVE-2024-29984, CVE-2024-29985

SQL Drivers

SQL Server, OLE DB Driver

CVE-2024-29045 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: Required
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-2024-21409 | .NET and Visual Studio Remote Code Execution Vulnerability

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

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

Affected Products: .NET 6.0, .NET 7.0, .NET 8.0, .NET Framework, Visual Studio 2022

Other Products

Azure Kubernetes

CVE-2024-29990 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Azure Kubernetes Service Confidential Containers

Other Products

Azure Monitor Agent

CVE-2024-29989 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.4
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure Monitor Agent

Other Products

Outlook for Windows

CVE-2024-20670 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Outlook for Windows

Other Products

Azure

CVE-2024-20685 Azure Private 5G Core

CVE-2024-21322/21323/21324/29053/29054/29055 Defender for IoT

CVE-2024-21424 Azure Compute Gallery

CVE-2024-26193 Azure Migrate

CVE-2024-28917 Azure Arc

CVE-2024-29063 Azure AI Search

CVE-2024-29992 Azure Identity Library for .NET

CVE-2024-29993 Azure CycleCloud

Product Lifecycle Update

Fixed Policy

Visual Studio 2013
Visual Studio Team Foundation Server 2013

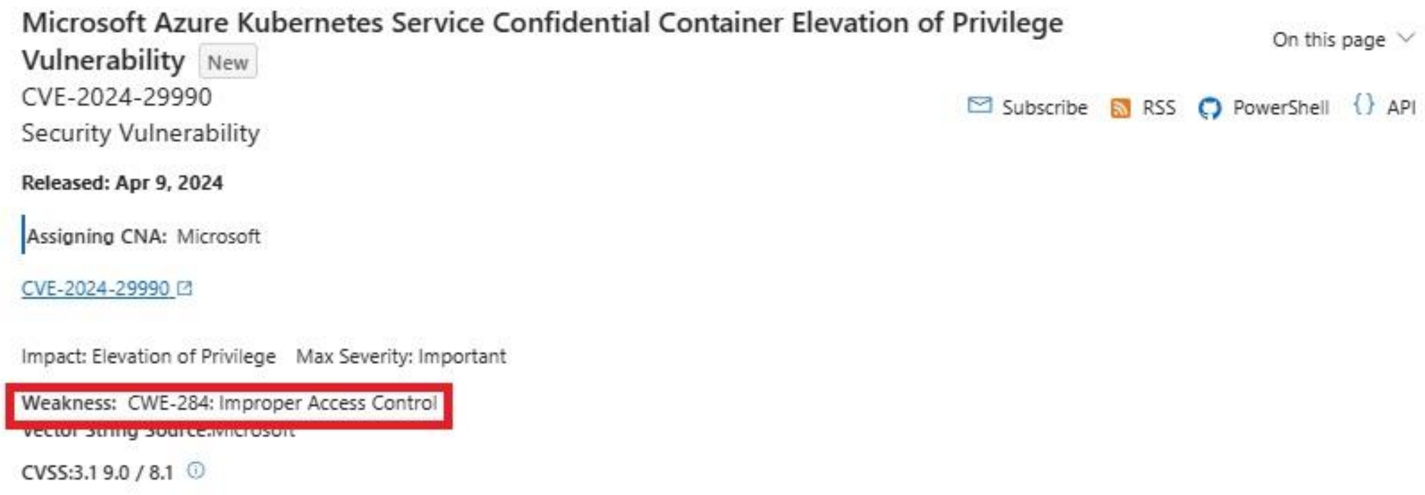
Modern Policy

Dynamics 365 Business Central on-premises (Modern Policy), 2022 release wave 2, version 21.x

aka.ms/lifecycle

Latest Servicing Stack Updates

Toward greater transparency: Adopting the CWE standard for Microsoft CVEs



Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability New

CVE-2024-29990

Security Vulnerability

Released: Apr 9, 2024

Assigning CNA: Microsoft

CVE-2024-29990

Impact: Elevation of Privilege Max Severity: Important

Weakness: CWE-284: Improper Access Control

Vector String Source:Microsoft

CVSS:3.1 9.0 / 8.1

- 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-2024-20669	No	No	Secure Boot
CVE-2024-20688	No	No	Secure Boot
CVE-2024-20689	No	No	Secure Boot
CVE-2024-26250	No	No	Secure Boot
CVE-2024-26252	No	No	rndismp6.sys
CVE-2024-26253	No	No	rndismp6.sys
CVE-2024-26254	No	No	Virtual Machine Bus (VMBus)
CVE-2024-26255	No	No	Remote Access Connection Manager
CVE-2024-26256	No	No	libarchive
CVE-2024-26172	No	No	DWM Core Library
CVE-2024-26179	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-26200	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-26205	No	No	Routing and Remote Access Service (RRAS)
CVE-2024-26232	No	No	Message Queuing (MSMQ)

CVE	Public	Exploited	Product
CVE-2024-28920	No	No	Secure Boot
CVE-2024-28922	No	No	Secure Boot
CVE-2024-28921	No	No	Secure Boot
CVE-2024-28919	No	No	Secure Boot
CVE-2024-28923	No	No	Secure Boot
CVE-2024-28896	No	No	Secure Boot
CVE-2024-28898	No	No	Secure Boot
CVE-2024-28901	No	No	Remote Access Connection Manager
CVE-2024-28902	No	No	Remote Access Connection Manager
CVE-2024-28903	No	No	Secure Boot
CVE-2024-29050	No	No	Cryptographic Services
CVE-2024-29064	No	No	Hyper-V
CVE-2024-29066	No	No	Distributed File System (DFS)
CVE-2024-23594	No	No	Lenovo: CVE-2024-23594 Stack Buffer Overflow in LenovoBT.efi

CVE	Public	Exploited	Product
CVE-2024-20678	No	No	Remote Procedure Call Runtime
CVE-2024-20665	No	No	BitLocker
CVE-2024-20693	No	No	Kernel
CVE-2024-21447	No	No	Authentication
CVE-2024-26168	No	No	Secure Boot
CVE-2024-26171	No	No	Secure Boot
CVE-2024-26175	No	No	Secure Boot
CVE-2024-26180	No	No	Secure Boot
CVE-2024-26183	No	No	Kerberos
CVE-2024-26189	No	No	Secure Boot
CVE-2024-26194	No	No	Secure Boot
CVE-2024-26195	No	No	DHCP Server Service
CVE-2024-26202	No	No	DHCP Server Service
CVE-2024-26209	No	No	Local Security Authority Subsystem Service

CVE	Public	Exploited	Product
CVE-2024-26218	No	No	Kernel
CVE-2024-26219	No	No	HTTP.sys
CVE-2024-26220	No	No	Mobile Hotspot
CVE-2024-26221	No	No	DNS Server
CVE-2024-26222	No	No	DNS Server
CVE-2024-26223	No	No	DNS Server
CVE-2024-26224	No	No	DNS Server
CVE-2024-26227	No	No	DNS Server
CVE-2024-26231	No	No	DNS Server
CVE-2024-26233	No	No	DNS Server
CVE-2024-26241	No	No	Win32k
CVE-2024-26243	No	No	USB Print Driver
CVE-2024-26248	No	No	Kerberos
CVE-2024-26229	No	No	CSC Service

CVE	Public	Exploited	Product
CVE-2024-26234	Yes	Yes	Proxy Driver
CVE-2024-26235	No	No	Update Stack
CVE-2024-26236	No	No	Update Stack
CVE-2024-26237	No	No	Defender Credential Guard
CVE-2024-26242	No	No	Telephony Server
CVE-2024-26245	No	No	SMB
CVE-2024-26207	No	No	Remote Access Connection Manager
CVE-2024-26208	No	No	Message Queuing (MSMQ)
CVE-2024-26211	No	No	Remote Access Connection Manager
CVE-2024-26212	No	No	DHCP Server Service
CVE-2024-26215	No	No	DHCP Server Service
CVE-2024-26216	No	No	File Server Resource Management Service
CVE-2024-26217	No	No	Remote Access Connection Manager
CVE-2024-26226	No	No	Distributed File System (DFS)

CVE	Public	Exploited	Product
CVE-2024-26228	No	No	Cryptographic Services
CVE-2024-26230	No	No	Telephony Server
CVE-2024-26239	No	No	Telephony Server
CVE-2024-26240	No	No	Secure Boot
CVE-2024-28924	No	No	Secure Boot
CVE-2024-28925	No	No	Secure Boot
CVE-2024-28897	No	No	Secure Boot
CVE-2024-28900	No	No	Remote Access Connection Manager
CVE-2024-29052	No	No	Storage
CVE-2024-29056	No	No	Authentication
CVE-2024-29061	No	No	Secure Boot
CVE-2024-29062	No	No	Secure Boot
CVE-2024-20670	No	No	Outlook for
CVE-2024-23593	No	No	Lenovo: CVE-2024-23593 Zero Out Boot Manager and drop to UEFI Shell

CVE	Public	Exploited	Product
CVE-2024-3156	No	No	Chromium: CVE-2024-3156 Inappropriate implementation in V8
CVE-2024-3158	No	No	Chromium: CVE-2024-3158 Use after free in Bookmarks
CVE-2024-3159	No	No	Chromium: CVE-2024-3159 Out of bounds memory access in V8
CVE-2024-29981	No	No	Edge (Chromium-based)
CVE-2024-29049	No	No	Edge (Chromium-based) Webview2
CVE-2024-26251	No	No	SharePoint Server
CVE-2024-26257	No	No	Excel
CVE-2024-21409	No	No	.NET, .NET Framework, and Visual Studio
CVE-2024-21424	No	No	Azure Compute Gallery
CVE-2024-26158	No	No	Install Service
CVE-2024-28905	No	No	Brokering File System
CVE-2024-28906	No	No	OLE DB Driver for SQL Server
CVE-2024-28908	No	No	OLE DB Driver for SQL Server
CVE-2024-28909	No	No	OLE DB Driver for SQL Server

CVE	Public	Exploited	Product
CVE-2024-28910	No	No	OLE DB Driver for SQL Server
CVE-2024-28911	No	No	OLE DB Driver for SQL Server
CVE-2024-28912	No	No	OLE DB Driver for SQL Server
CVE-2024-28913	No	No	OLE DB Driver for SQL Server
CVE-2024-28914	No	No	OLE DB Driver for SQL Server
CVE-2024-28915	No	No	OLE DB Driver for SQL Server
CVE-2024-28929	No	No	ODBC Driver for SQL Server
CVE-2024-28931	No	No	ODBC Driver for SQL Server
CVE-2024-28932	No	No	ODBC Driver for SQL Server
CVE-2024-28936	No	No	ODBC Driver for SQL Server
CVE-2024-28939	No	No	OLE DB Driver for SQL Server
CVE-2024-28942	No	No	OLE DB Driver for SQL Server
CVE-2024-28945	No	No	OLE DB Driver for SQL Server
CVE-2024-29043	No	No	ODBC Driver for SQL Server

CVE	Public	Exploited	Product
CVE-2024-29045	No	No	OLE DB Driver for SQL Server
CVE-2024-29047	No	No	OLE DB Driver for SQL Server
CVE-2024-29063	No	No	Azure AI Search
CVE-2024-20685	No	No	Azure Private 5G Core
CVE-2024-29988	No	No	SmartScreen Prompt
CVE-2024-29990	No	No	Azure Kubernetes Service Confidential Container
CVE-2024-2201	No	No	Intel: CVE-2024-2201 Branch History Injection
CVE-2024-21322	No	No	Defender for IoT
CVE-2024-21323	No	No	Defender for IoT
CVE-2024-21324	No	No	Defender for IoT
CVE-2024-26193	No	No	Azure Migrate
CVE-2024-26210	No	No	WDAC OLE DB Provider for SQL Server
CVE-2024-26244	No	No	WDAC OLE DB Provider for SQL Server
CVE-2024-26213	No	No	Brokering File System

CVE	Public	Exploited	Product
CVE-2024-26214	No	No	WDAC SQL Server ODBC Driver
CVE-2024-28904	No	No	Brokering File System
CVE-2024-28907	No	No	Brokering File System
CVE-2024-28917	No	No	Azure Arc-enabled Kubernetes Extension Cluster-Scope
CVE-2024-28926	No	No	OLE DB Driver for SQL Server
CVE-2024-28927	No	No	OLE DB Driver for SQL Server
CVE-2024-28930	No	No	ODBC Driver for SQL Server
CVE-2024-28933	No	No	ODBC Driver for SQL Server
CVE-2024-28934	No	No	ODBC Driver for SQL Server
CVE-2024-28935	No	No	ODBC Driver for SQL Server
CVE-2024-28937	No	No	ODBC Driver for SQL Server
CVE-2024-28938	No	No	ODBC Driver for SQL Server
CVE-2024-28940	No	No	OLE DB Driver for SQL Server
CVE-2024-28941	No	No	ODBC Driver for SQL Server

CVE	Public	Exploited	Product
CVE-2024-28943	No	No	ODBC Driver for SQL Server
CVE-2024-28944	No	No	OLE DB Driver for SQL Server
CVE-2024-29044	No	No	OLE DB Driver for SQL Server
CVE-2024-29046	No	No	OLE DB Driver for SQL Server
CVE-2024-29048	No	No	OLE DB Driver for SQL Server
CVE-2024-29053	No	No	Defender for IoT
CVE-2024-29055	No	No	Defender for IoT
CVE-2024-29054	No	No	Defender for IoT
CVE-2024-29982	No	No	OLE DB Driver for SQL Server
CVE-2024-29983	No	No	OLE DB Driver for SQL Server
CVE-2024-29984	No	No	OLE DB Driver for SQL Server
CVE-2024-29985	No	No	OLE DB Driver for SQL Server
CVE-2024-29989	No	No	Azure Monitor Agent
CVE-2024-29992	No	No	Azure Identity Library for .NET

CVE	Public	Exploited	Product
CVE-2024-29993	No	No	Azure CycleCloud