Microsoft

Microsoft Security Release

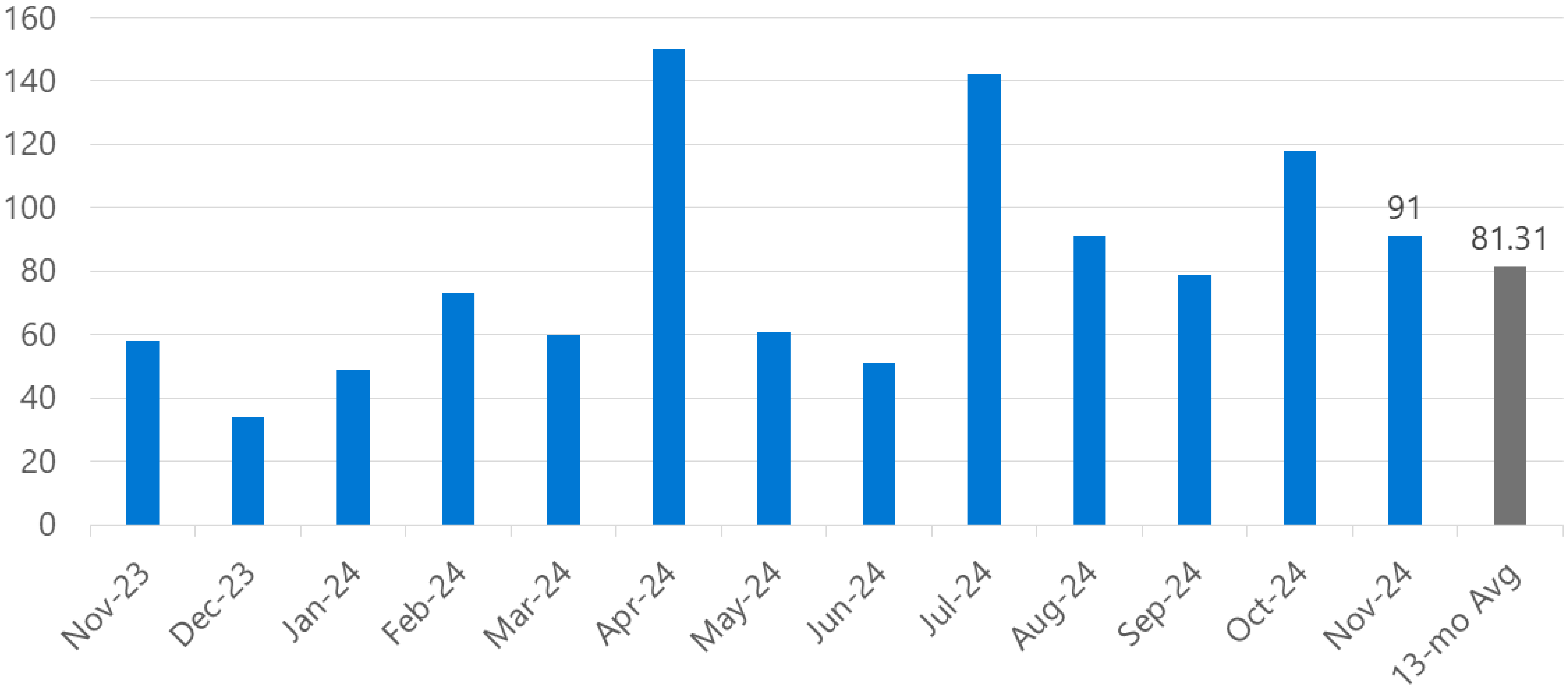
November 12, 2024

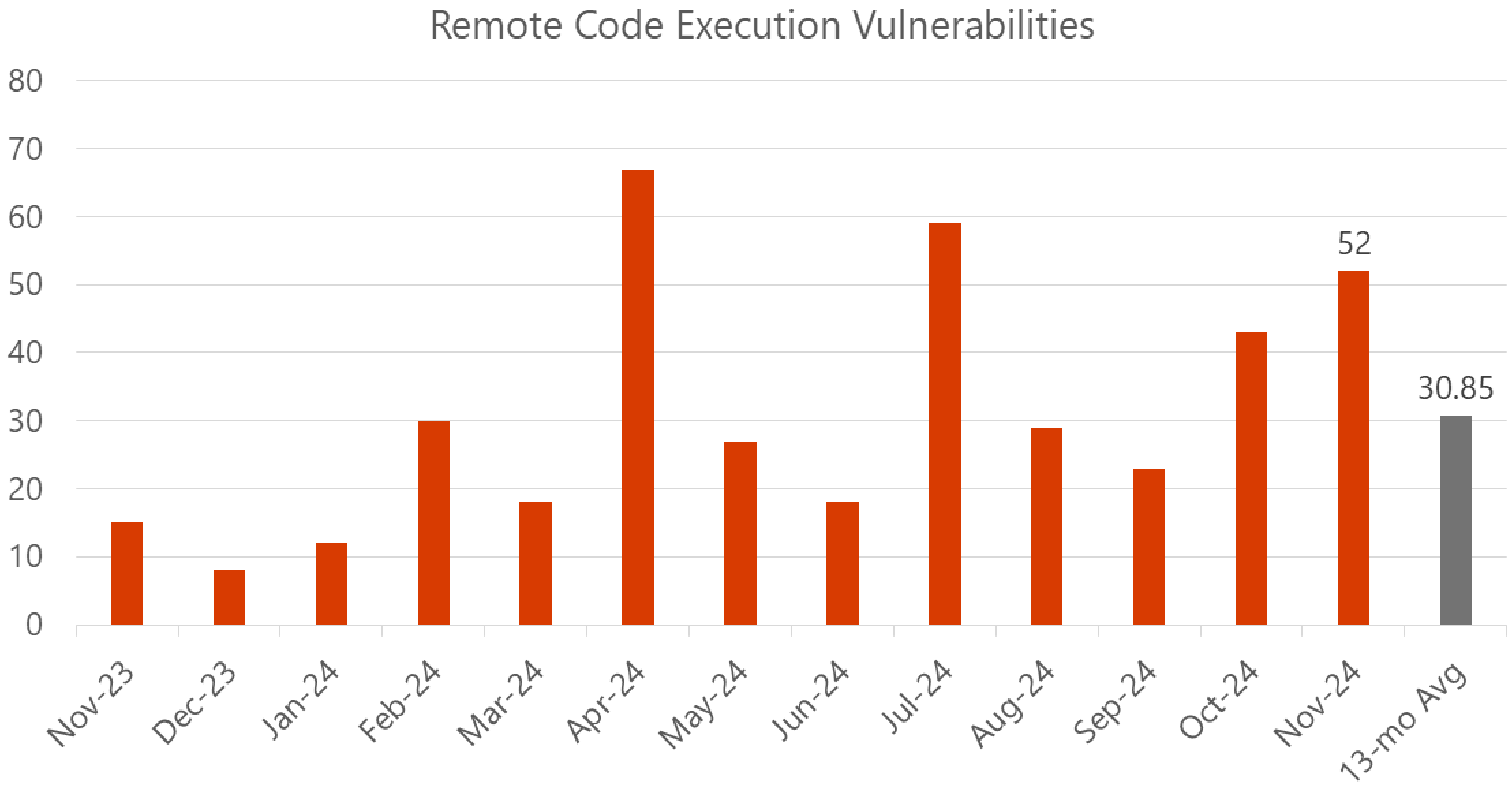
Agenda

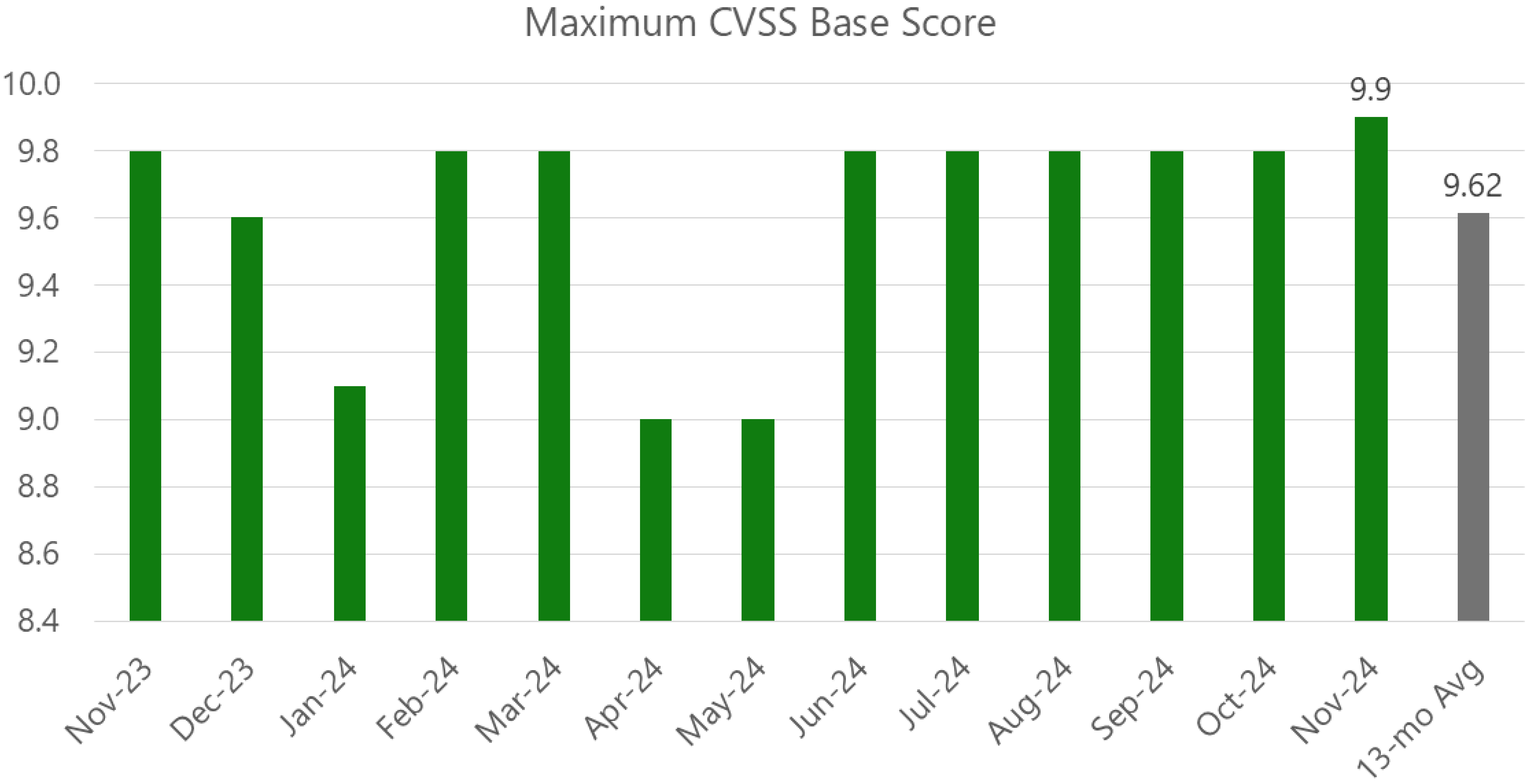
- Security Updates
- Security Advisory
- Product Support Lifecyle

Microsoft

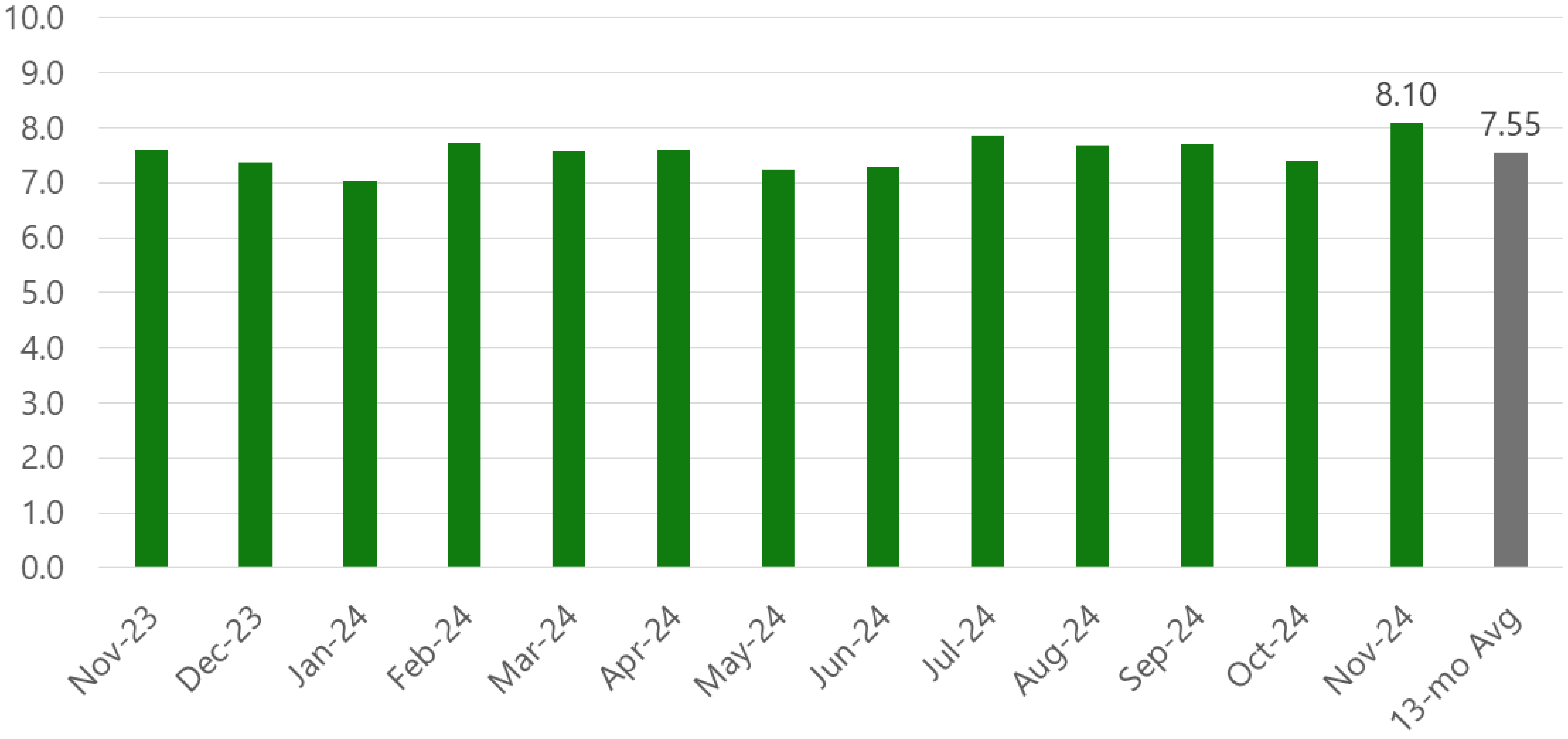
Vulnerabilities per month



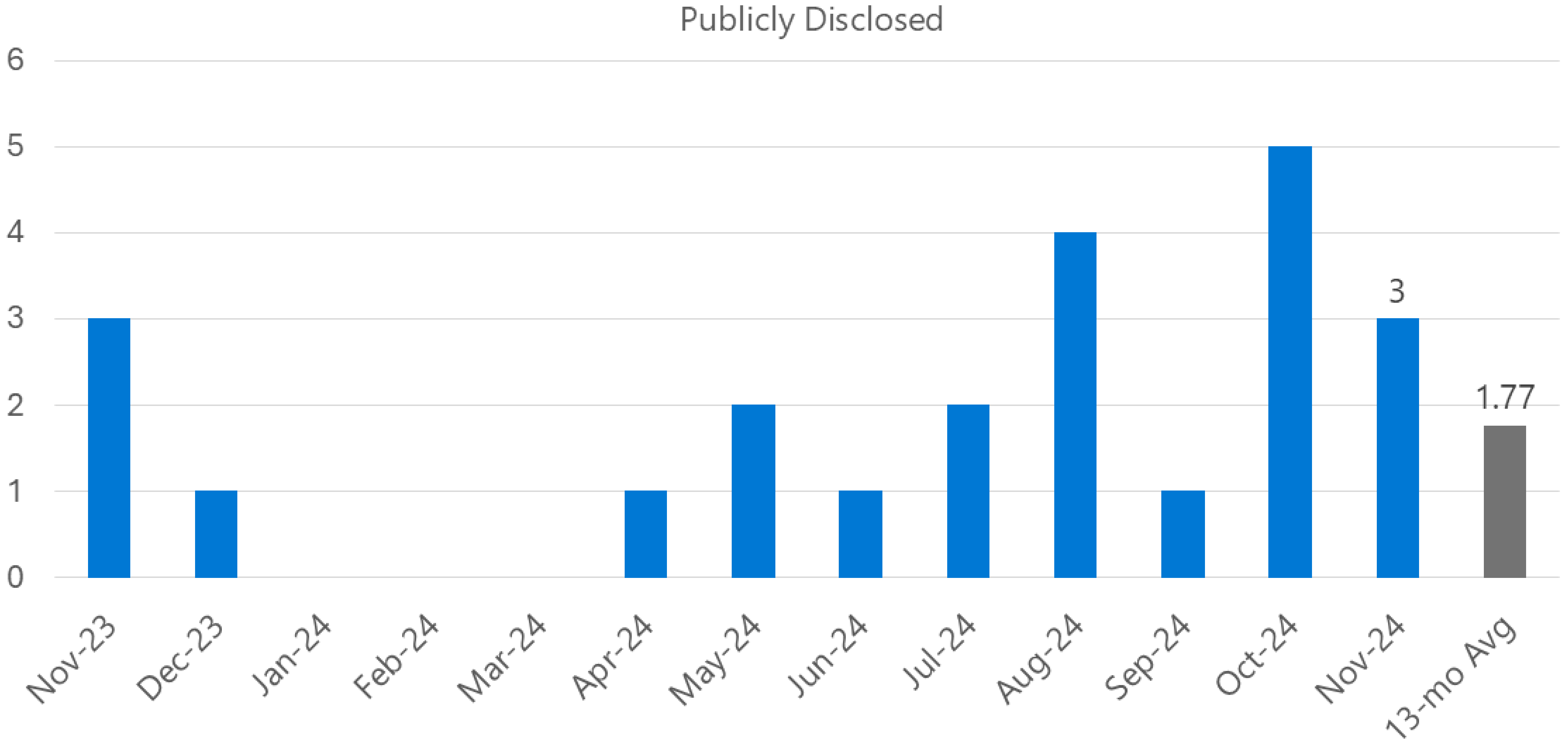

Remote Code Execution Vulnerabilities
80
70
60
50
40
30
20
10
0
52
30.85
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
13-mo Avg


Maximum CVSS Base Score
10.0
9.8
9.6
9.4
9.2
9.0
8.8
8.6
8.4
9.9
9.62
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
13-mo Avg

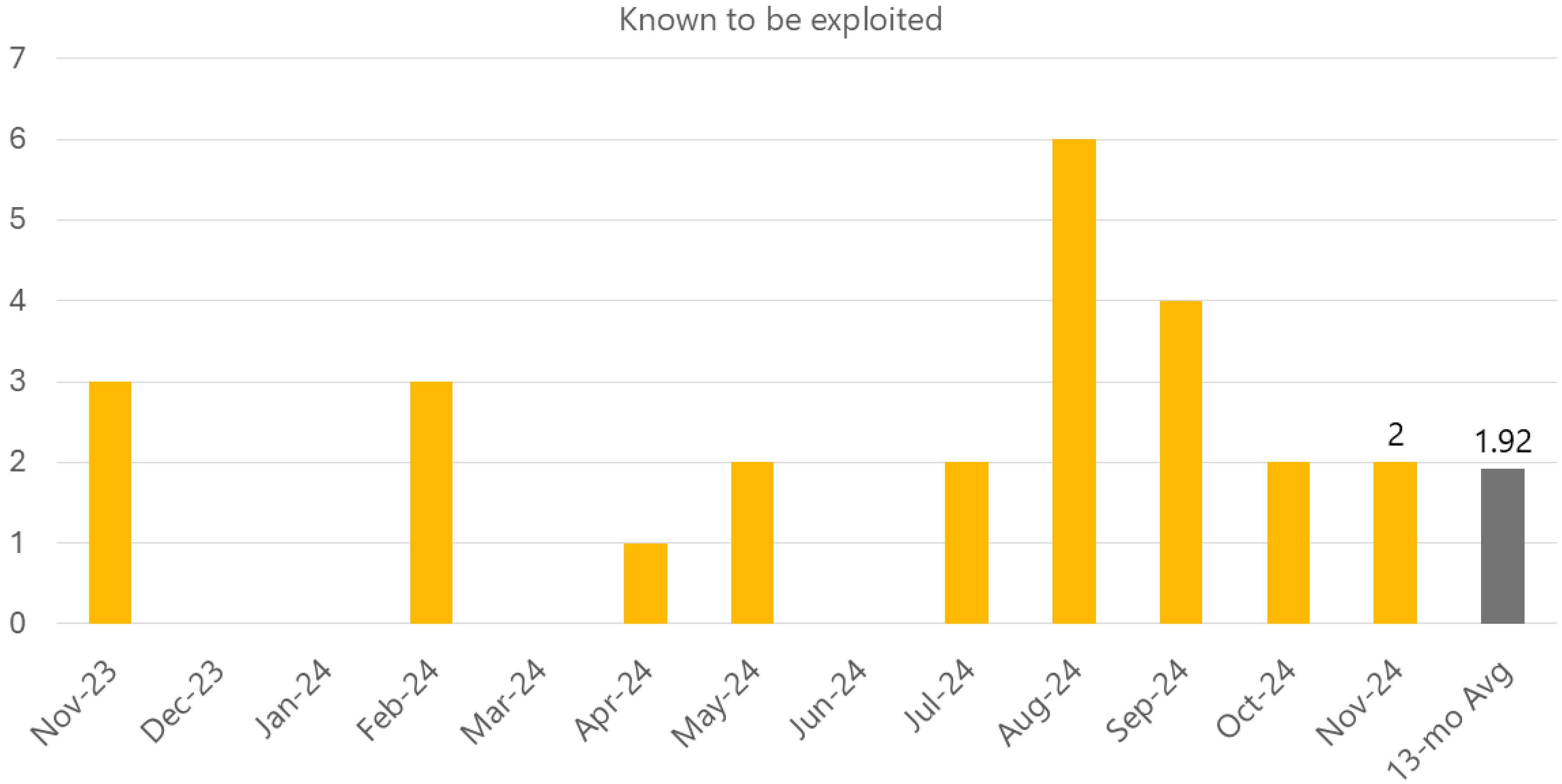
Average CVSS Base Score



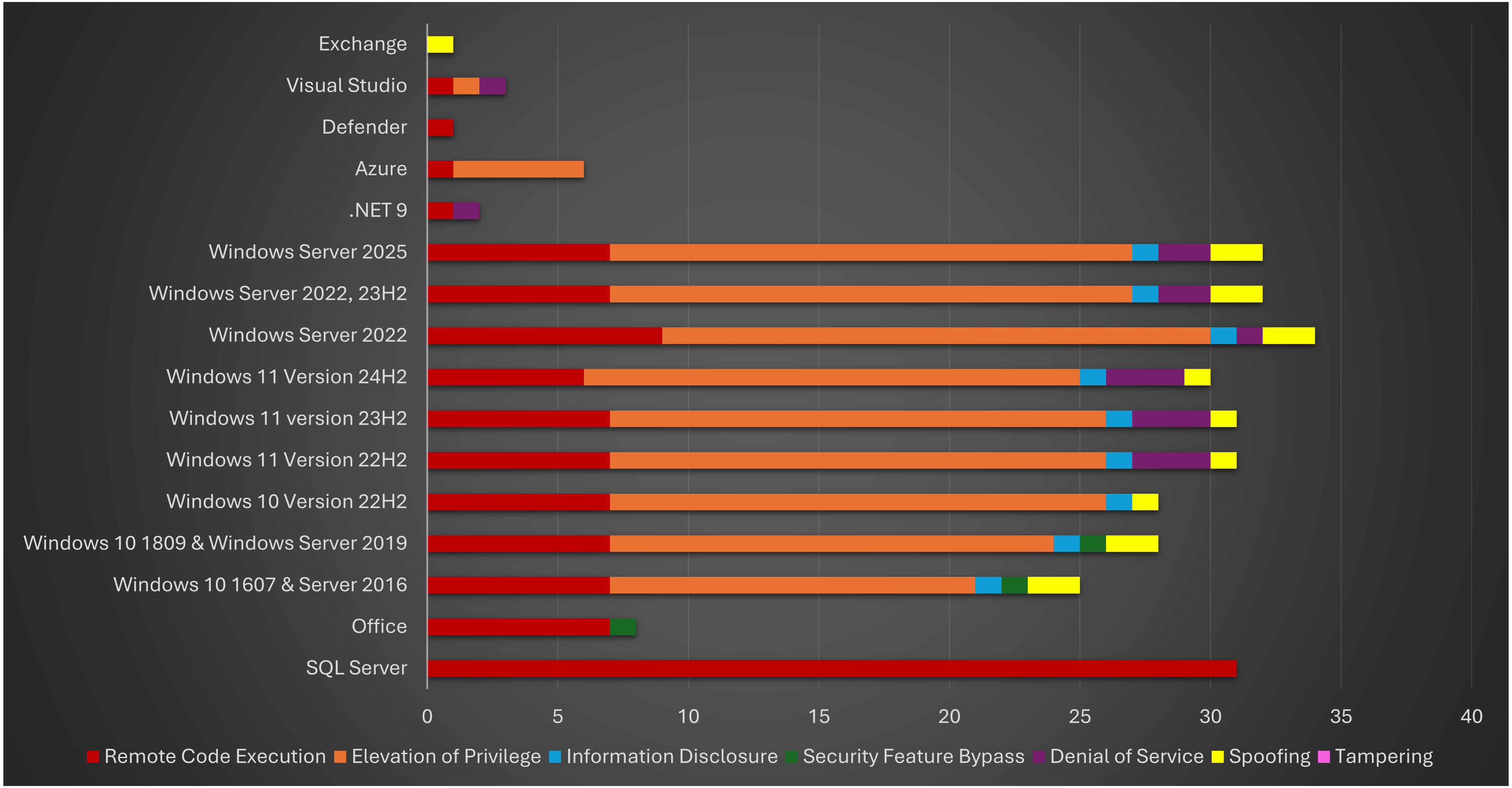
Microsoft


Publicly Disclosed
6
5
4
3
2
1
0
3
1.77
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
13-mo Avg

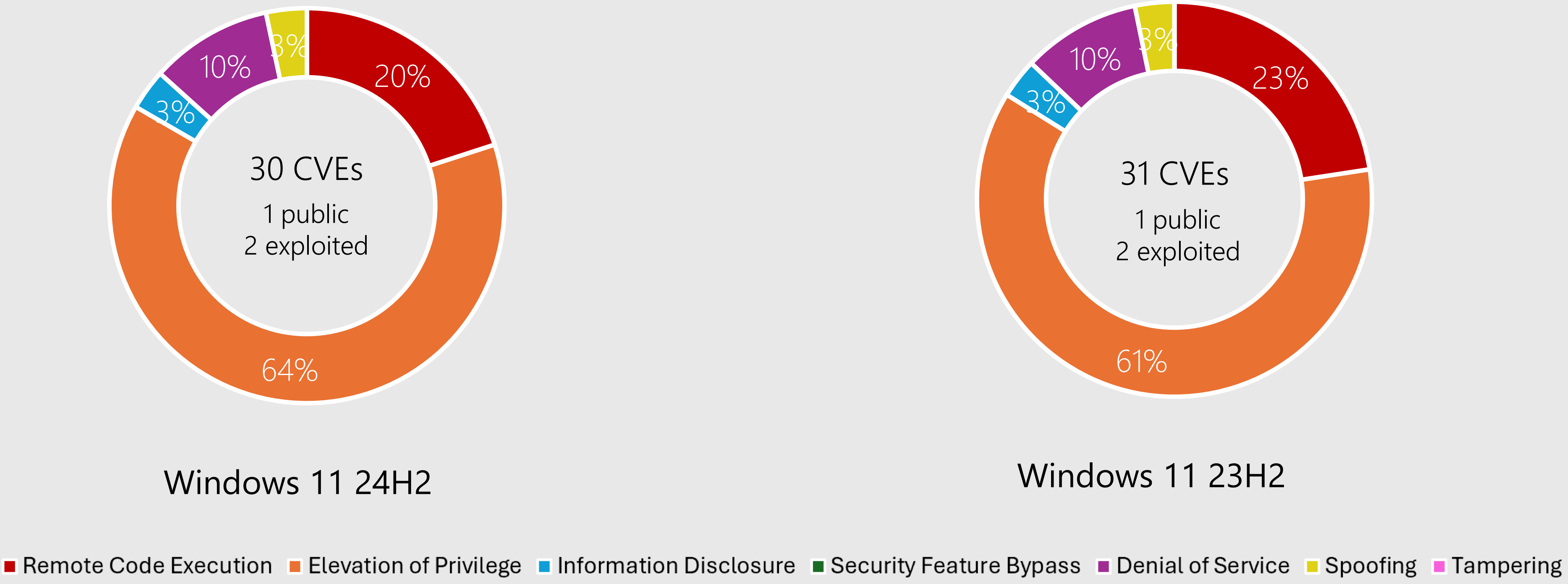
Microsoft


Known to be exploited
7
6
5
4
3
2
1
0
2
1.92
Nov-23
Dec-23
Jan-24
Feb-24
Mar-24
Apr-24
May-24
Jun-24
Jul-24
Aug-24
Sep-24
Oct-24
Nov-24
13-mo Avg

Microsoft Security Release Overview – November 2024

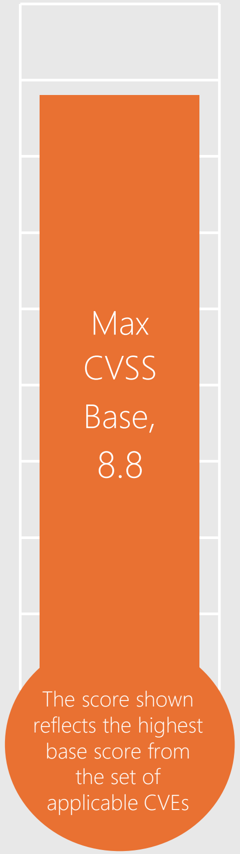


Windows 11



Windows 11 24H2

Windows 11 23H2



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

Affected Components:

See Appendix for details

CVE-2024-49039 Task Scheduler

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

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 2025
Server 2022
Server 2019
Server 2016

CVE-2024-43451 NTLM

Impact, Severity, Disclosure

Spoofing | Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 6.5 | 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 2025
Server 2022
Server 2019
Server 2016

CVE-2024-43625 Windows VMSwitch

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.1 | Attack Vector: Local | Attack Complexity: High | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

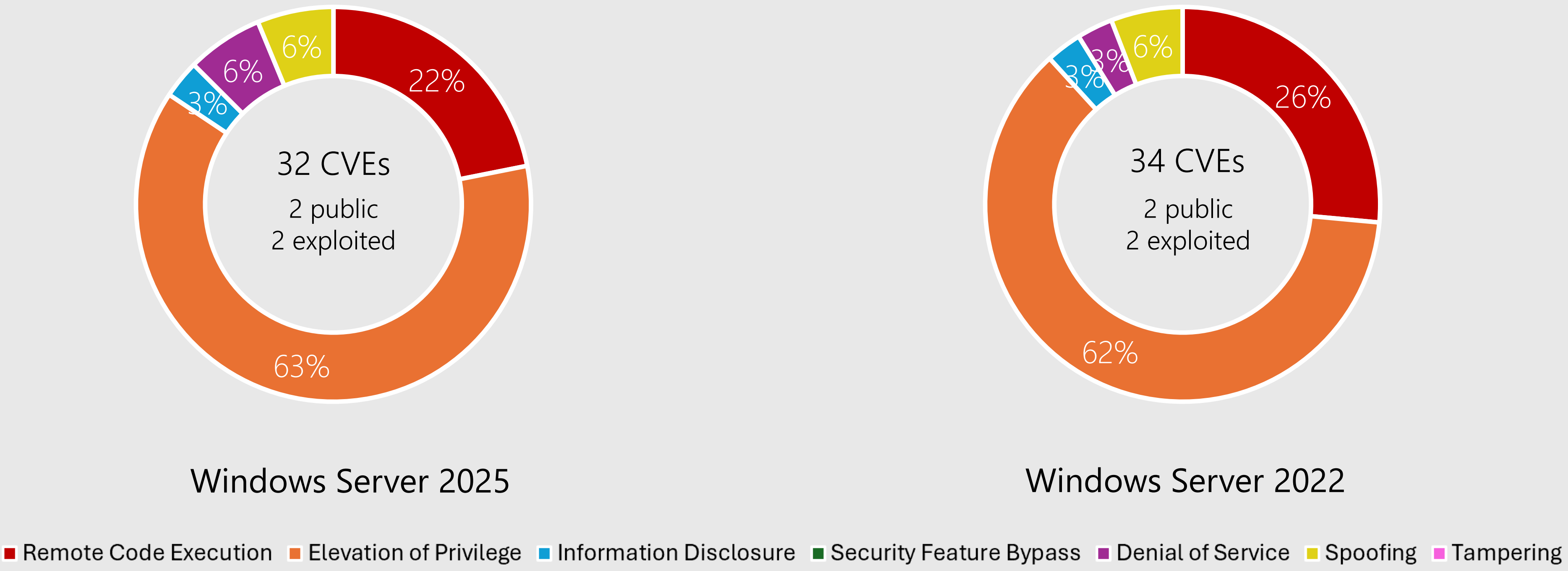
Workarounds

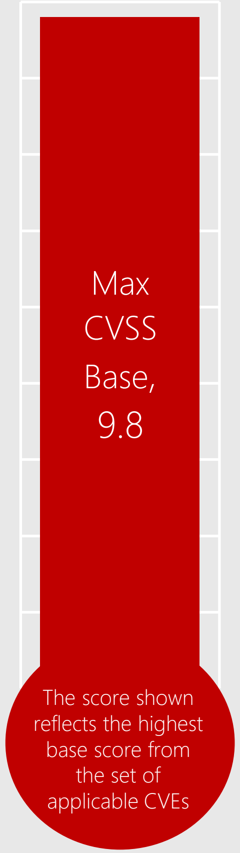
Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Server 2025
Server 2022

Server 2025, 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-2024-43639 Kerberos

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

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2025
Server 2022
Server 2019
Server 2016

CVE-2024-43447 SMB

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.

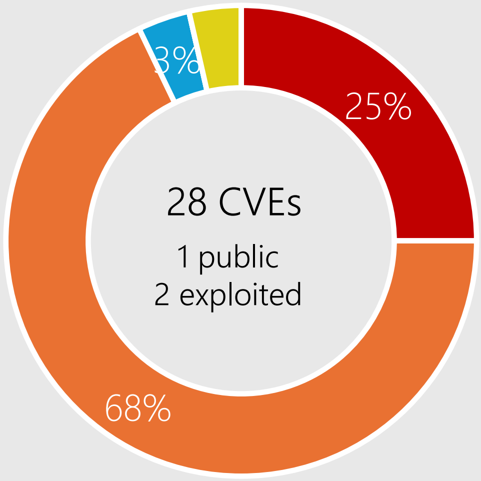
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

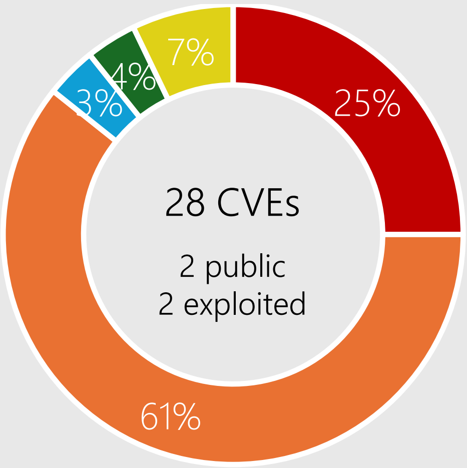
Affected Software

Server 2022

Windows 10



Windows 10 22H2



Windows 1809 & Server 2019

🟥 Remote Code Execution 🟧 Elevation of Privilege 🟦 Information Disclosure 🟩 Security Feature Bypass 🟪 Denial of Service 🟨 Spoofing ■ Tampering

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-2024-43627 Telephony 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: 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 2025
Server 2022
Server 2019
Server 2016

CVE-2024-43624 Hyper-V

Impact, Severity, Disclosure

Elevation of Privilege | 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 2025
Server 2022
Server 2019

CVE-2024-49019 AD Certificate Services

Impact, Severity, Disclosure

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

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.

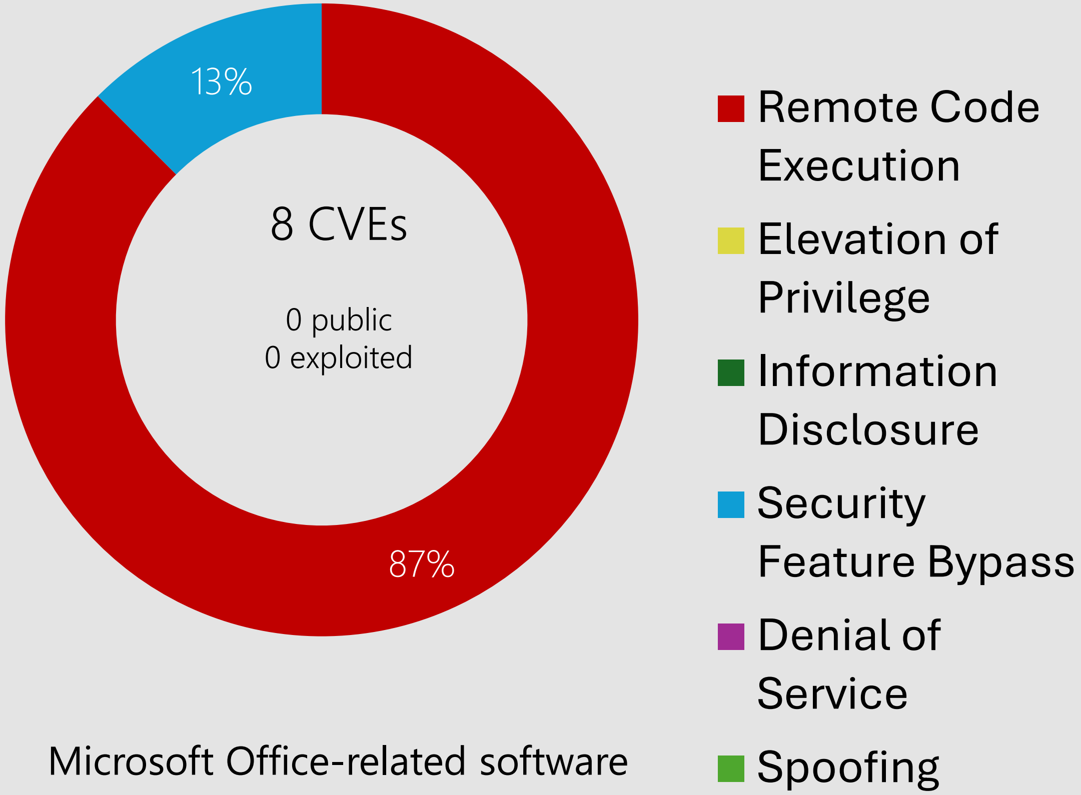
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2025
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
Office 2016
Excel 2016
Word 2016
365 Apps Enterprise
Office LTSC 2021
Office LTSC 2024

CVE-2024-49027 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 2019
Excel 2016
Office 365 Apps for Enterprise
Office LTSC 2021/2024

Exchange

Exchange

CVE-2024-49040 | Important | Spoofing | Public: Yes | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Microsoft Exchange Server 2016, Exchange 2019

SQL Server & Drivers

29 CVEs | SQL Server Native Client 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**: Yes
Affected Products: SQL Server 2019, SQL Server 2017, SQL Server 2016

CVE-2024-49021 | SQL Server Remote Code Execution Vulnerability

Base CVSS: 7.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No

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

CVE-2024-49043 | Microsoft.SqlServer.XEvent.Configuration.dll RCE Vulnerability

Base CVSS: 7.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No

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

Developer Tools

Microsoft .NET, Visual Studio

CVE-2024-43498 | .NET and Visual Studio Remote Code Execution Vulnerability

Base CVSS: 9.8 | **Max Severity**: Critical | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: NET 9.0, Visual Studio 2022

CVE-2024-43499 | .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 9.0, Visual Studio 2022

CVE-2024-49044 | Visual Studio Elevation of Privilege Vulnerability

Base CVSS: 6.7 | **Max Severity**: Important | **Public**: No | **Exploited**: No

Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: Low | **User Interaction Required**: Yes
Affected Products: Visual Studio 2022

Developer Tools

Visual Studio Code

CVE-2024-49049 | Visual Studio Code Elevation of Privilege Vulnerability

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

Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None

Affected Products: Visual Studio Code – Remote SSH extension

CVE-2024-49050 | Visual Studio Code Python Extension 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**: Yes

Affected Products: Python extension for Visual Studio Code

Other Products

Defender for Endpoint

CVE-2024-5535 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Microsoft Defender for Endpoint

Other Products

Azure, Apps, GitHub Projects

CVE-2024-43602 Azure CycleCloud

CVE-2024-49056 Airlift.microsoft.com

CVE-2024-43613/49042 Azure Database for PostgreSQL

CVE-2024-43598 LightGBM

CVE-2024-49051 Microsoft PC Manager

CVE-2024-49048 TorchGeo

Advisory – SharePoint Server Defense in Depth

Summary

Microsoft has released a security update for Microsoft SharePoint Server. The update provides a defense in depth enhancement regarding redirections.

Recommended Actions:

Apply the November 2024 SharePoint updates.

https://msrc.microsoft.com/update-guide/advisory/ADV240001

Product Lifecycle Update

Products reaching end of servicing in November

PowerShell 7.2 (LTS)
.NET 6.0 (LTS)

aka.ms/lifecycle

Microsoft

Questions?

Appendix

CVE	Component	Public	Exploited
CVE-2024-38203 Windows Package Library Manager	Package Library Manager	No	No
CVE-2024-38255 SQL Server	SQL Server Native Client	No	No
CVE-2024-38264 Microsoft Virtual Hard Drive	Virtual Hard Disk (VHDX)	No	No
CVE-2024-43447 Windows SMBv3 Client/Server	SMBv3 Server	No	No
CVE-2024-43449 Windows USB Video Driver	USB Video Class System Driver	No	No
CVE-2024-43450 Microsoft Windows DNS	DNS	No	No
CVE-2024-43451 Windows NTLM	NTLM Hash Disclosure	Yes	Yes
CVE-2024-43452 Windows Registry	Registry	No	No
CVE-2024-43459 SQL Server	SQL Server Native Client	No	No
CVE-2024-43462 SQL Server	SQL Server Native Client	No	No
CVE-2024-43498 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-43499 .NET and Visual Studio	.NET and Visual Studio	No	No
CVE-2024-43530 Windows Update Stack	Update Stack	No	No
CVE-2024-43598 LightGBM	LightGBM	No	No
CVE-2024-43602 Azure CycleCloud	Azure CycleCloud	No	No
CVE-2024-43613 Azure Database for PostgreSQL	Azure Database for PostgreSQL Flexible Server Extension	No	No
CVE-2024-43620 Windows Telephony Service	Telephony Service	No	No

CVE	Component	Public	Exploited
CVE-2024-43621 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43622 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43623 Windows NT OS Kernel	NT OS Kernel	No	No
CVE-2024-43624 Role: Windows Hyper-V	Hyper-V Shared Virtual Disk	No	No
CVE-2024-43625 Windows VMSwitch	Windows VMSwitch	No	No
CVE-2024-43626 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43627 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43628 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43629 Windows DWM Core Library	DWM Core Library	No	No
CVE-2024-43630 Windows Kernel	Kernel	No	No
CVE-2024-43631 Windows Secure Kernel Mode	Secure Kernel Mode	No	No
CVE-2024-43633 Role: Windows Hyper-V	Hyper-V	No	No
CVE-2024-43634 Windows USB Video Driver	USB Video Class System Driver	No	No
CVE-2024-43635 Windows Telephony Service	Telephony Service	No	No
CVE-2024-43636 Windows DWM Core Library	Win32k	No	No
CVE-2024-43637 Windows USB Video Driver	USB Video Class System Driver	No	No
CVE-2024-43638 Windows USB Video Driver	USB Video Class System Driver	No	No

CVE	Component	Public	Exploited
CVE-2024-43639 Windows Kerberos	Kerberos	No	No
CVE-2024-43640 Windows Secure Kernel Mode	Kernel-Mode Driver Elevation of Privilege	No	No
CVE-2024-43641 Windows Registry	Registry	No	No
CVE-2024-43642 Windows SMB	SMB	No	No
CVE-2024-43643 Windows USB Video Driver	USB Video Class System Driver	No	No
CVE-2024-43644 Windows CSC Service	Client-Side Caching	No	No
CVE-2024-43645 Windows Defender Application Control (WDAC)	Defender Application Control (WDAC)	No	No
CVE-2024-43646 Windows Secure Kernel Mode	Secure Kernel Mode	No	No
CVE-2024-48993 SQL Server	SQL Server Native Client	No	No
CVE-2024-48994 SQL Server	SQL Server Native Client	No	No
CVE-2024-48995 SQL Server	SQL Server Native Client	No	No
CVE-2024-48996 SQL Server	SQL Server Native Client	No	No
CVE-2024-48997 SQL Server	SQL Server Native Client	No	No
CVE-2024-48998 SQL Server	SQL Server Native Client	No	No
CVE-2024-48999 SQL Server	SQL Server Native Client	No	No
CVE-2024-49000 SQL Server	SQL Server Native Client	No	No

CVE	Component	Public	Exploited
CVE-2024-49001 SQL Server	SQL Server Native Client	No	No
CVE-2024-49002 SQL Server	SQL Server Native Client	No	No
CVE-2024-49003 SQL Server	SQL Server Native Client	No	No
CVE-2024-49004 SQL Server	SQL Server Native Client	No	No
CVE-2024-49005 SQL Server	SQL Server Native Client	No	No
CVE-2024-49006 SQL Server	SQL Server Native Client	No	No
CVE-2024-49007 SQL Server	SQL Server Native Client	No	No
CVE-2024-49008 SQL Server	SQL Server Native Client	No	No
CVE-2024-49009 SQL Server	SQL Server Native Client	No	No
CVE-2024-49010 SQL Server	SQL Server Native Client	No	No
CVE-2024-49011 SQL Server	SQL Server Native Client	No	No
CVE-2024-49012 SQL Server	SQL Server Native Client	No	No
CVE-2024-49013 SQL Server	SQL Server Native Client	No	No
CVE-2024-49014 SQL Server	SQL Server Native Client	No	No
CVE-2024-49015 SQL Server	SQL Server Native Client	No	No
CVE-2024-49016 SQL Server	SQL Server Native Client	No	No

CVE	Component	Public	Exploited
CVE-2024-49017 SQL Server	SQL Server Native Client	No	No
CVE-2024-49018 SQL Server	SQL Server Native Client	No	No
CVE-2024-49019 Role: Windows Active Directory Certificate Services	Active Directory Certificate Services	Yes	No
CVE-2024-49021 SQL Server	SQL Server	No	No
CVE-2024-49026 Microsoft Office Excel	Excel	No	No
CVE-2024-49027 Microsoft Office Excel	Excel	No	No
CVE-2024-49028 Microsoft Office Excel	Excel	No	No
CVE-2024-49029 Microsoft Office Excel	Excel	No	No
CVE-2024-49030 Microsoft Office Excel	Excel	No	No
CVE-2024-49031 Microsoft Graphics Component	Office Graphics	No	No
CVE-2024-49032 Microsoft Graphics Component	Office Graphics	No	No
CVE-2024-49033 Microsoft Office Word	Word	No	No
CVE-2024-49039 Windows Task Scheduler	Task Scheduler	No	Yes
CVE-2024-49040 Microsoft Exchange Server	Exchange Server	Yes	No
CVE-2024-49042 Azure Database for PostgreSQL	Azure Database for PostgreSQL Flexible Server Extension	No	No
CVE-2024-49043 SQL Server	.SqlServer.XEvent.Configuration.dll	No	No

CVE	Component	Public	Exploited
CVE-2024-49044 Visual Studio	Visual Studio	No	No
CVE-2024-49046 Windows Win32 Kernel Subsystem	Win32 Kernel Subsystem	No	No
CVE-2024-49048 TorchGeo	TorchGeo	No	No
CVE-2024-49049 Visual Studio Code	Visual Studio Code Remote Extension	No	No
CVE-2024-49050 Visual Studio Code	Visual Studio Code Python Extension	No	No
CVE-2024-49051 Microsoft PC Manager	PC Manager	No	No
CVE-2024-49056 Airlift.microsoft.com	Airlift.microsoft.com	No	No
CVE-2024-5535 Microsoft Defender for Endpoint	OpenSSL: CVE-2024-5535 SSL_select_next_proto buffer overread	No	No