

# EMEA Security Briefing Call

May 15<sup>th</sup>, 2024

Faisal Hussain (Syd) 

Marc Alexander 

Microsoft EMEA Security Program Management

On Demand Recording of the Webcast available at <https://aka.ms/EMEAWebcastMay>  
This presentation deck available for download at <https://aka.ms/EMEADeckMay>



# Agenda



Security Updates

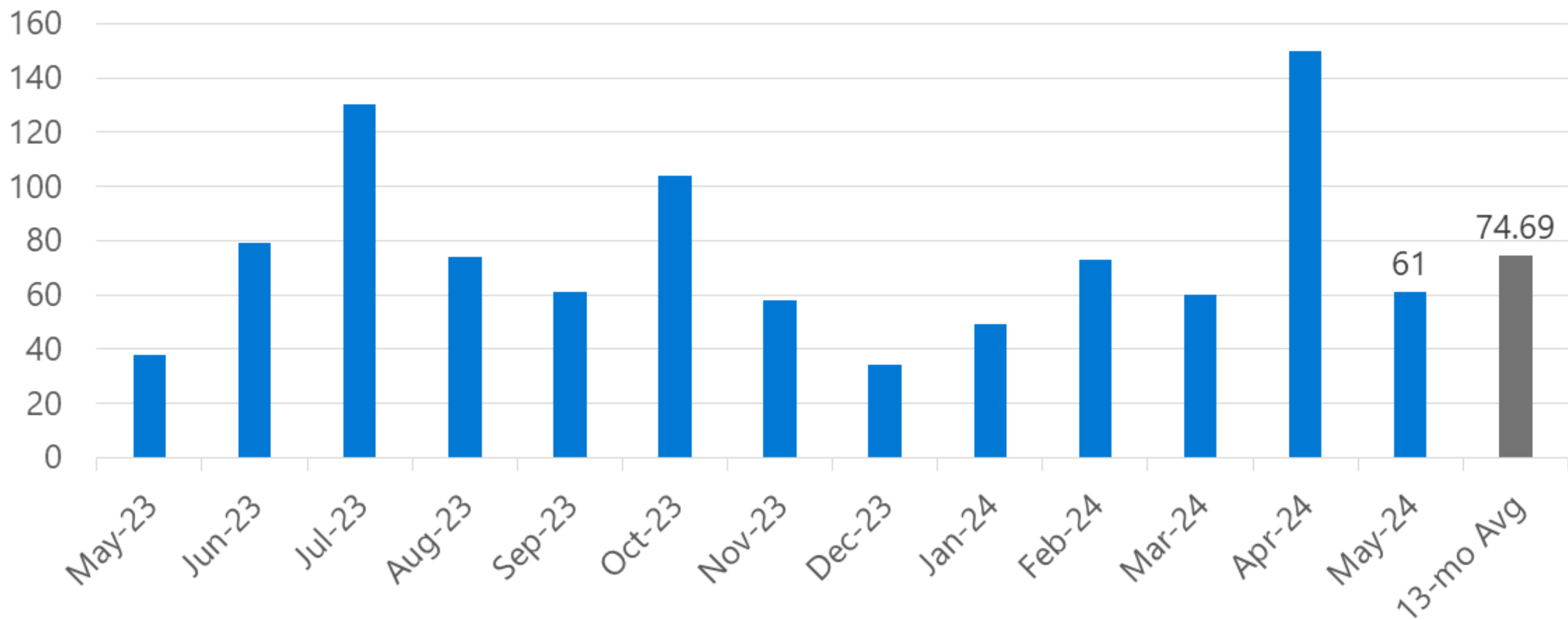


Product Support Lifecycle

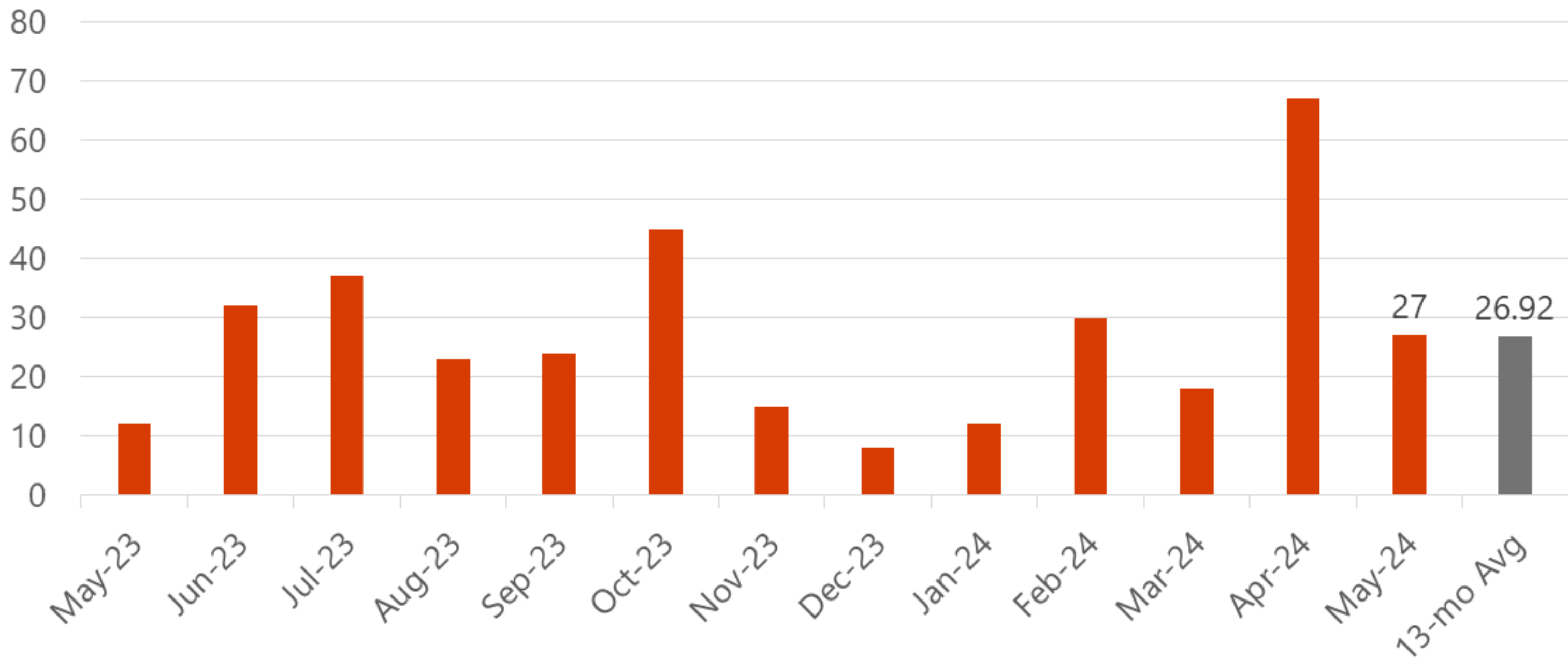


Other resources related to the release

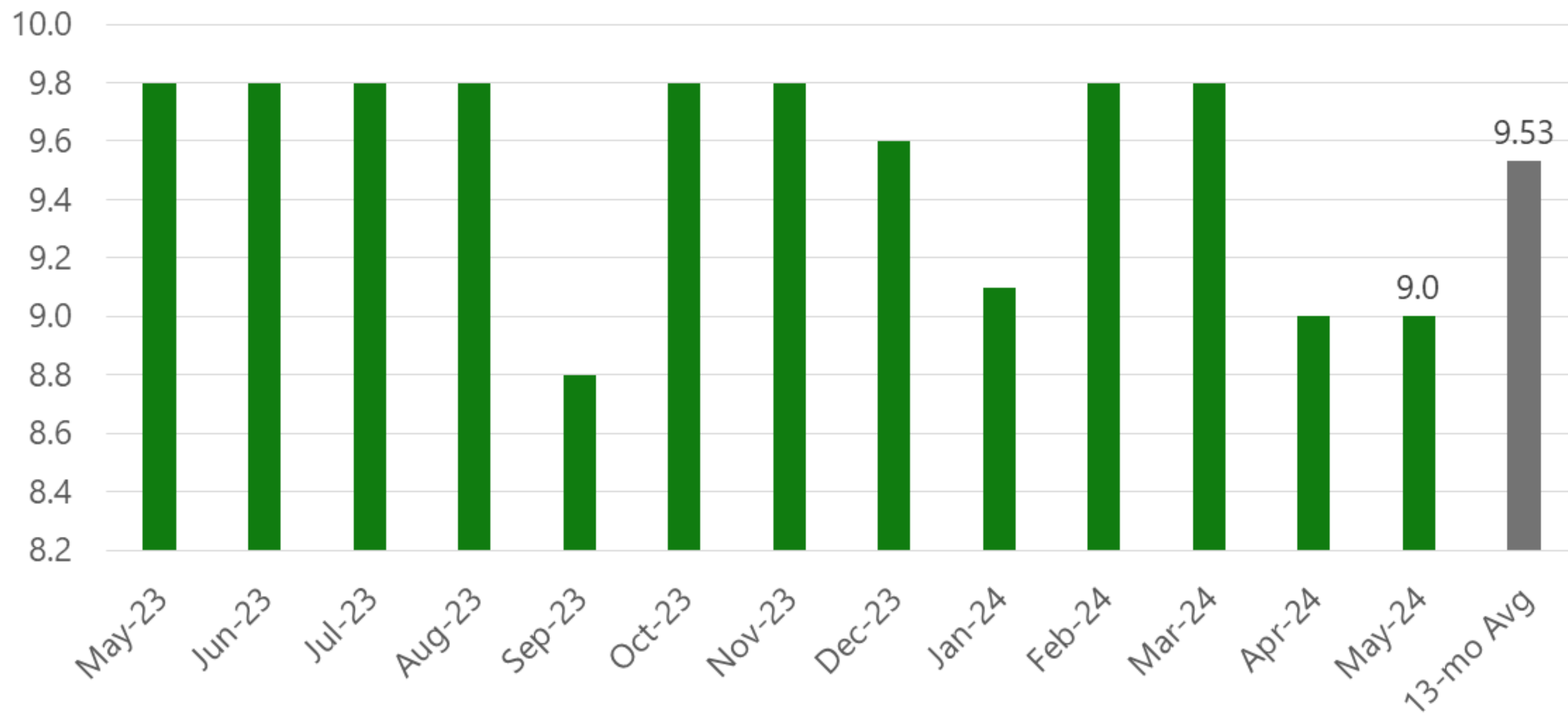
## Vulnerabilities per month



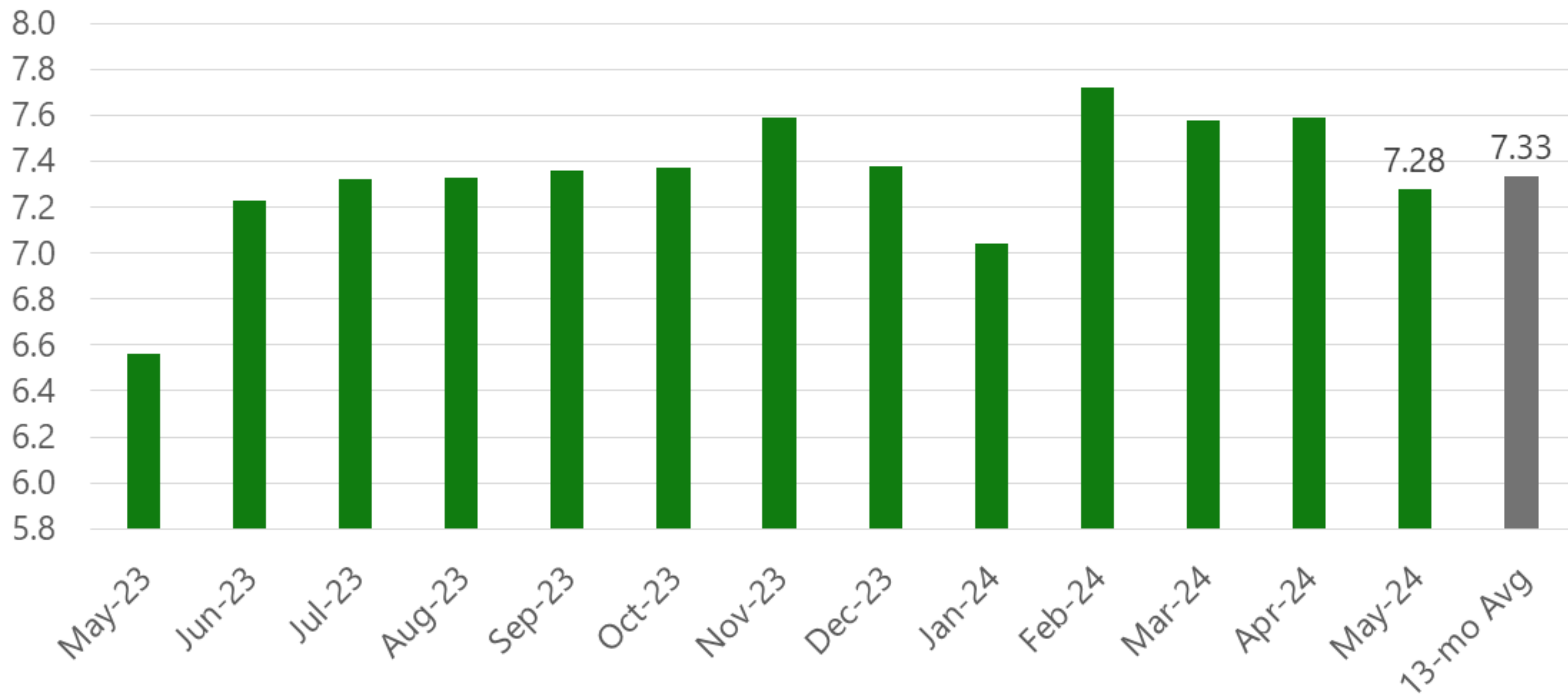
## Remote Code Execution Vulnerabilities



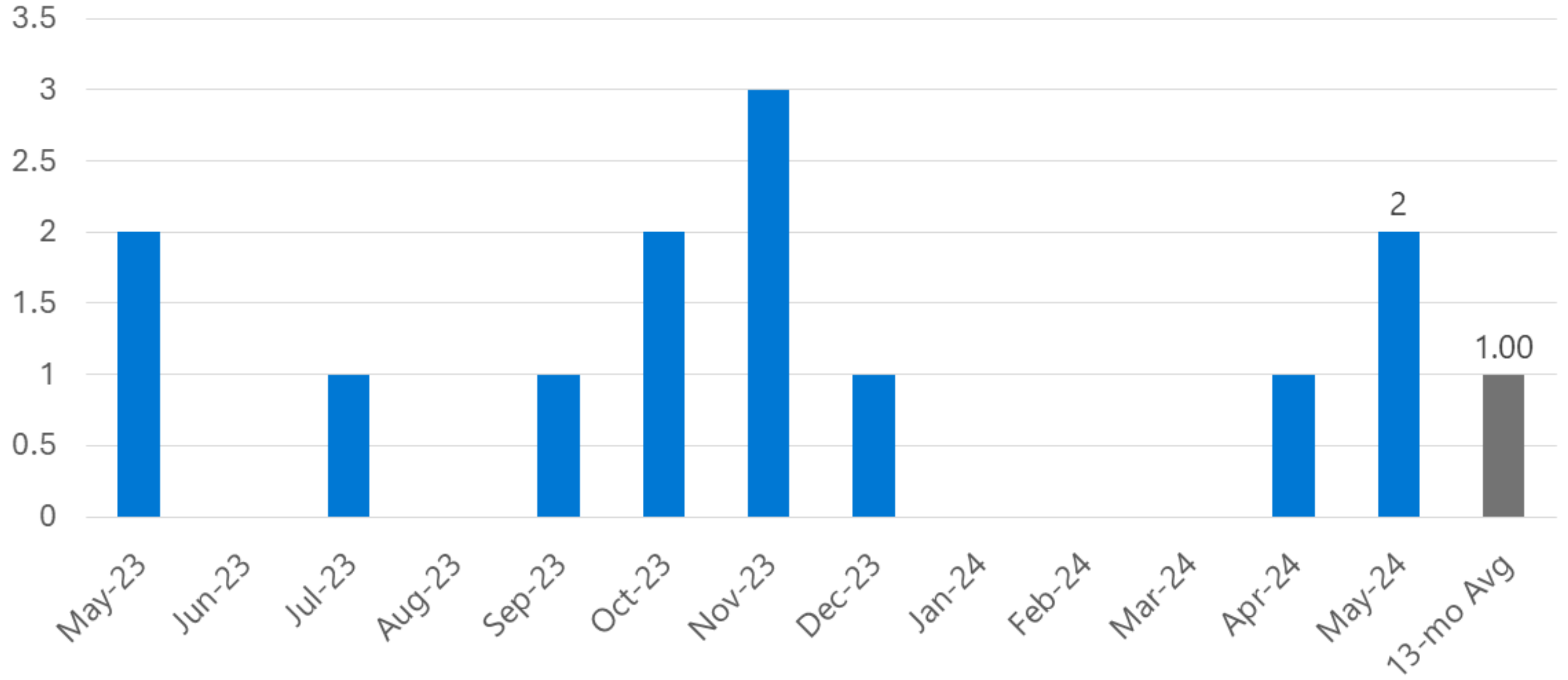
## Maximum CVSS Base Score



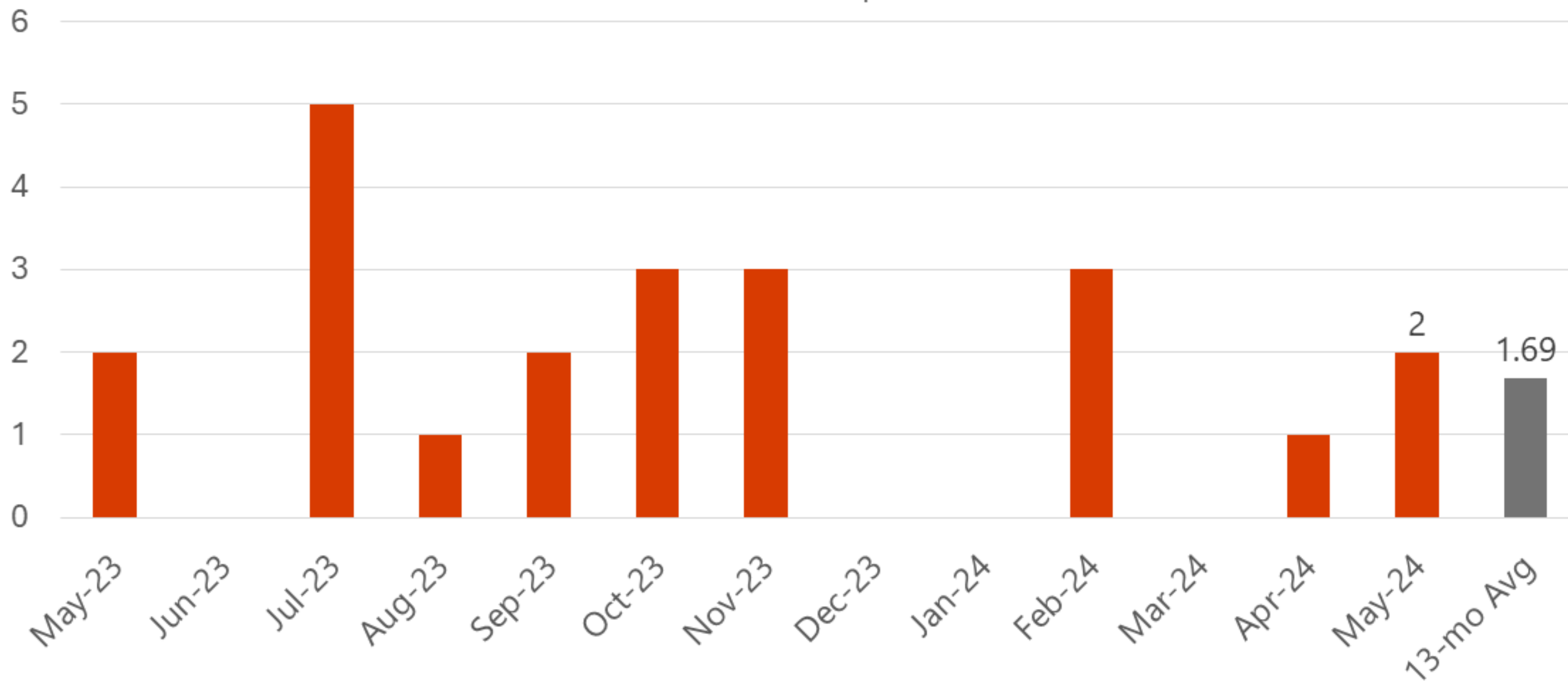
## Average CVSS Base Score



Publicly Disclosed

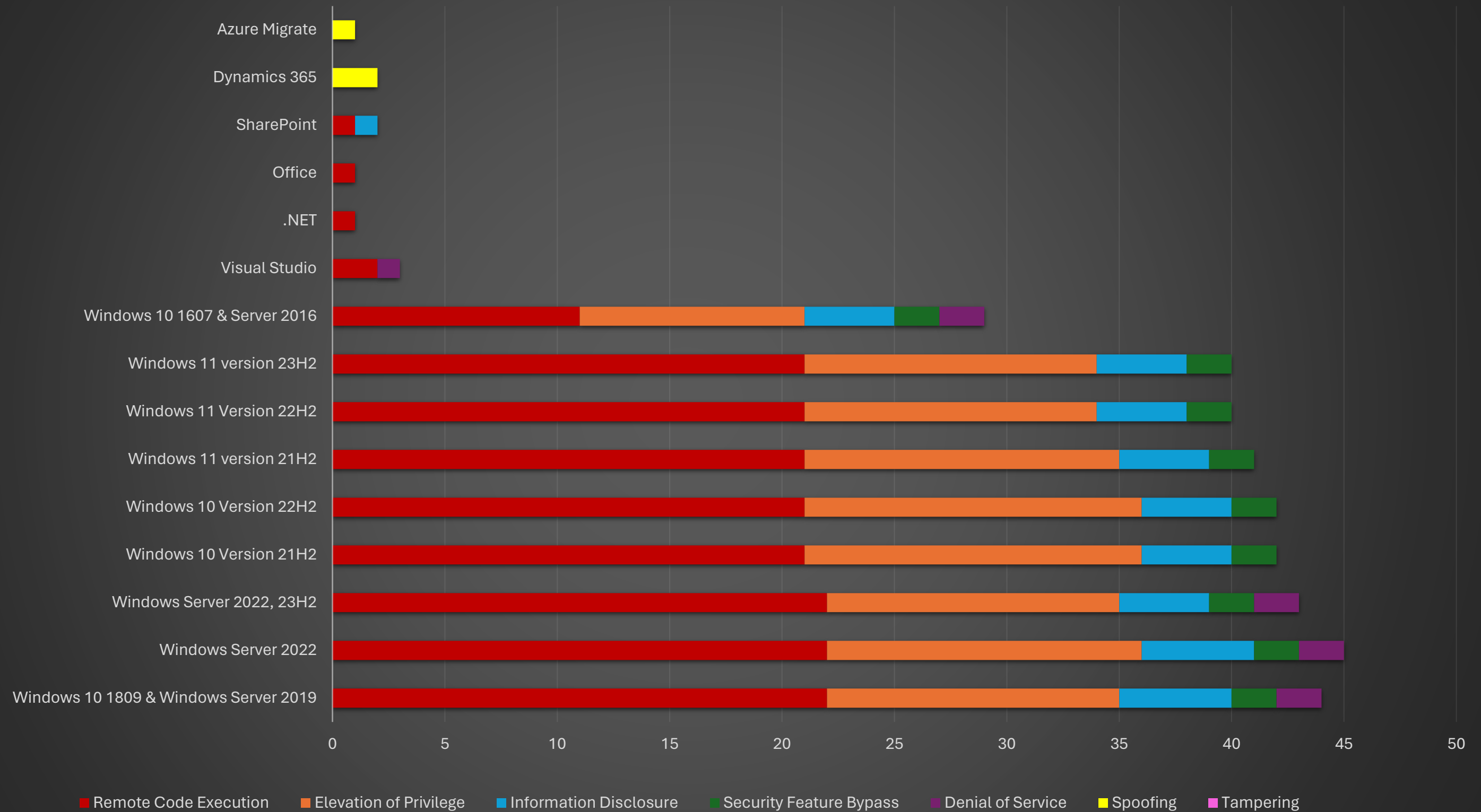


Known to be exploited

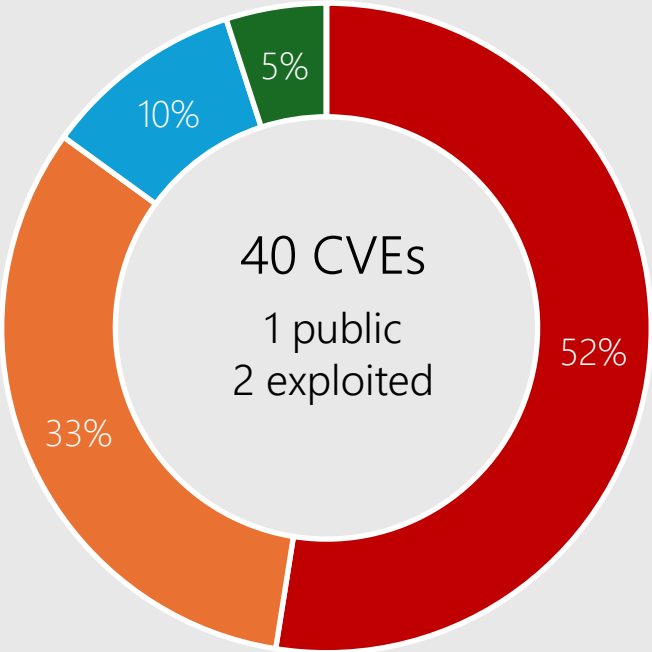




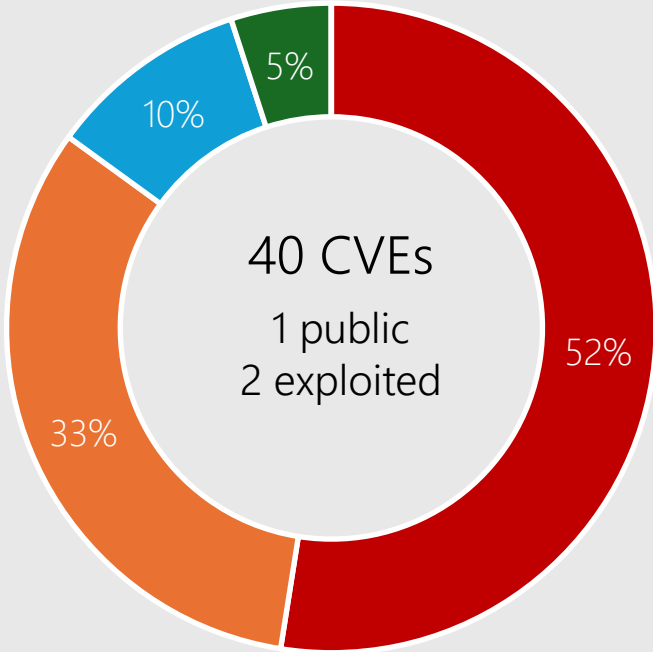
# Microsoft Security Release Overview – May 2024



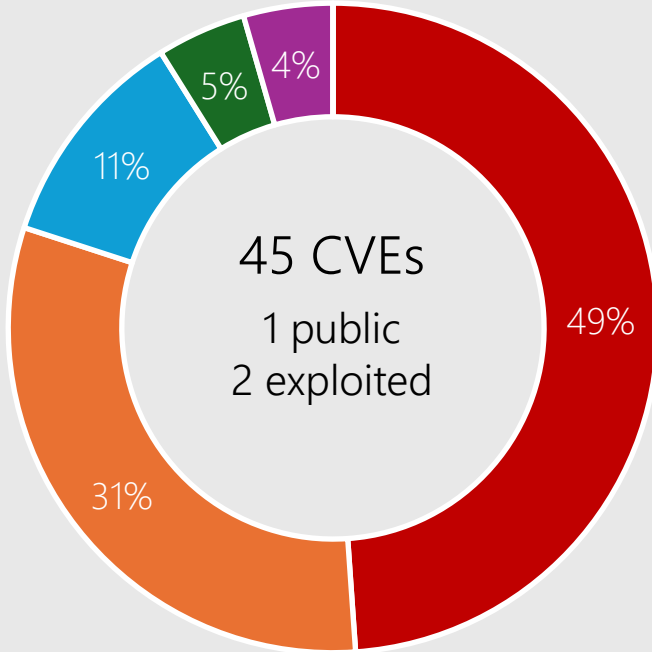
# Windows 11, Server 2022



Windows 11 23H2

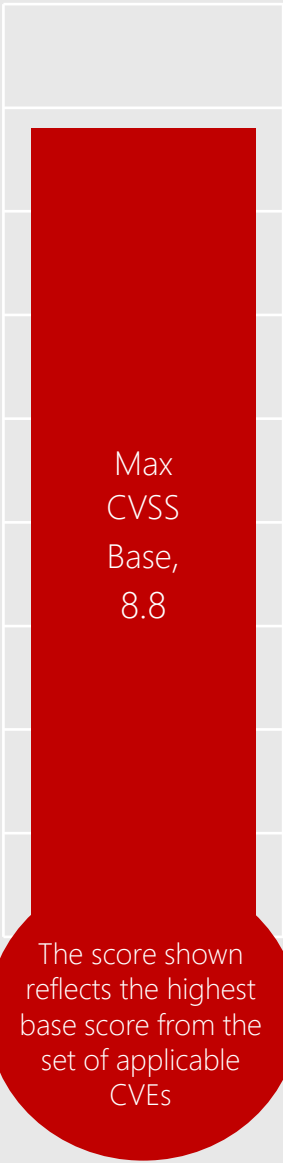


Windows 11 22H2



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



## CVSS Score Metrics

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



## CVSS Score Metrics

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

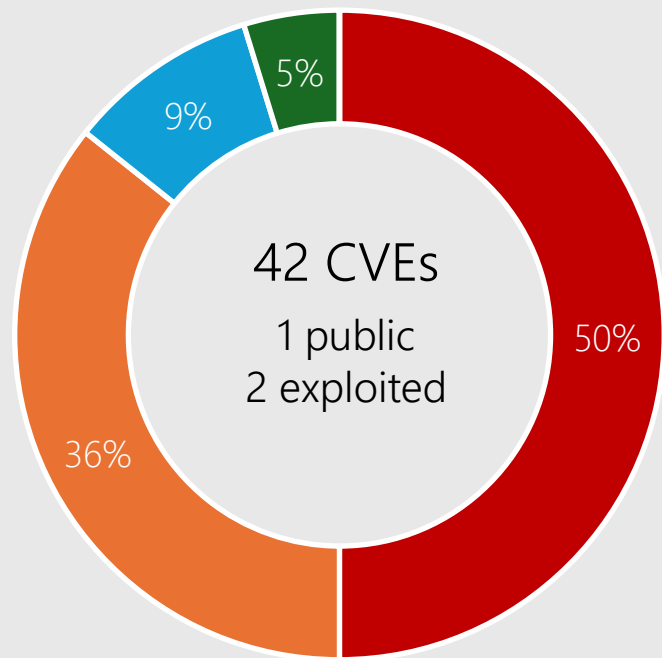
Microsoft has not identified any workarounds for this vulnerability.

# Affected Software

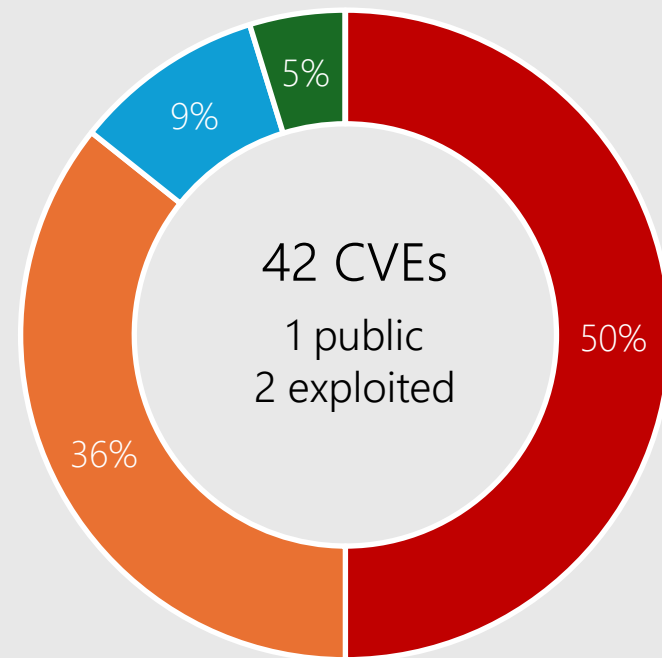


Server 2022, 23H2

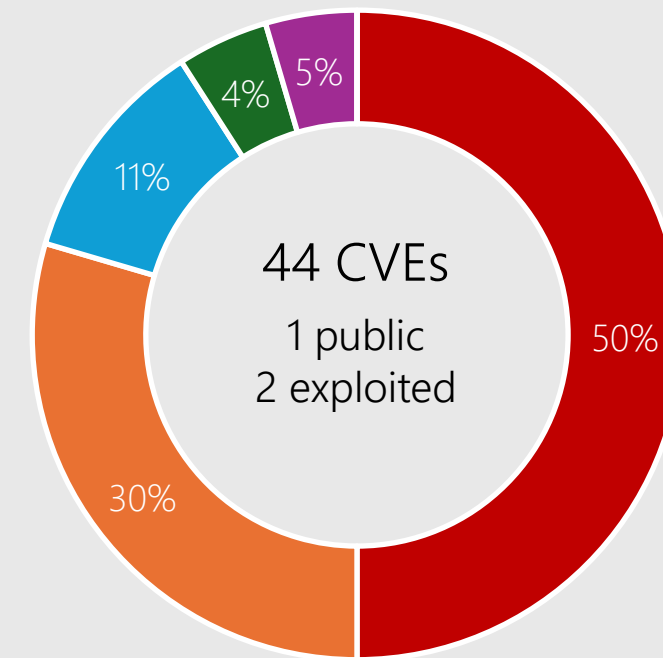
# Windows 10



Windows 10 22H2

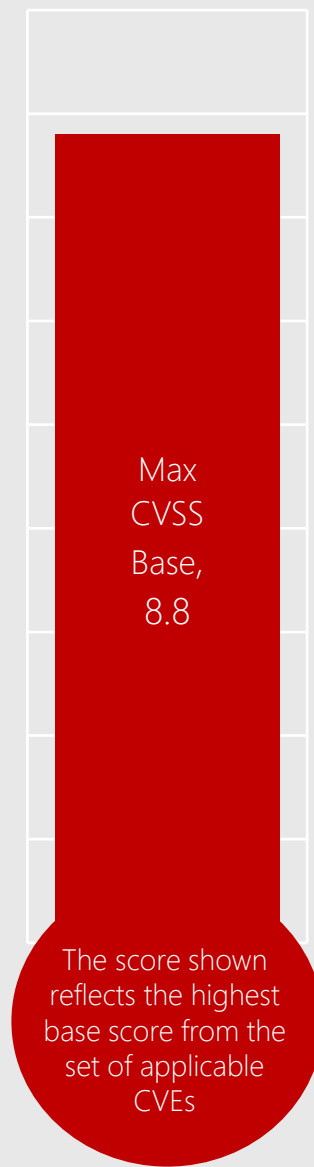


Windows 10 21H2



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



## CVSS Score Metrics

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

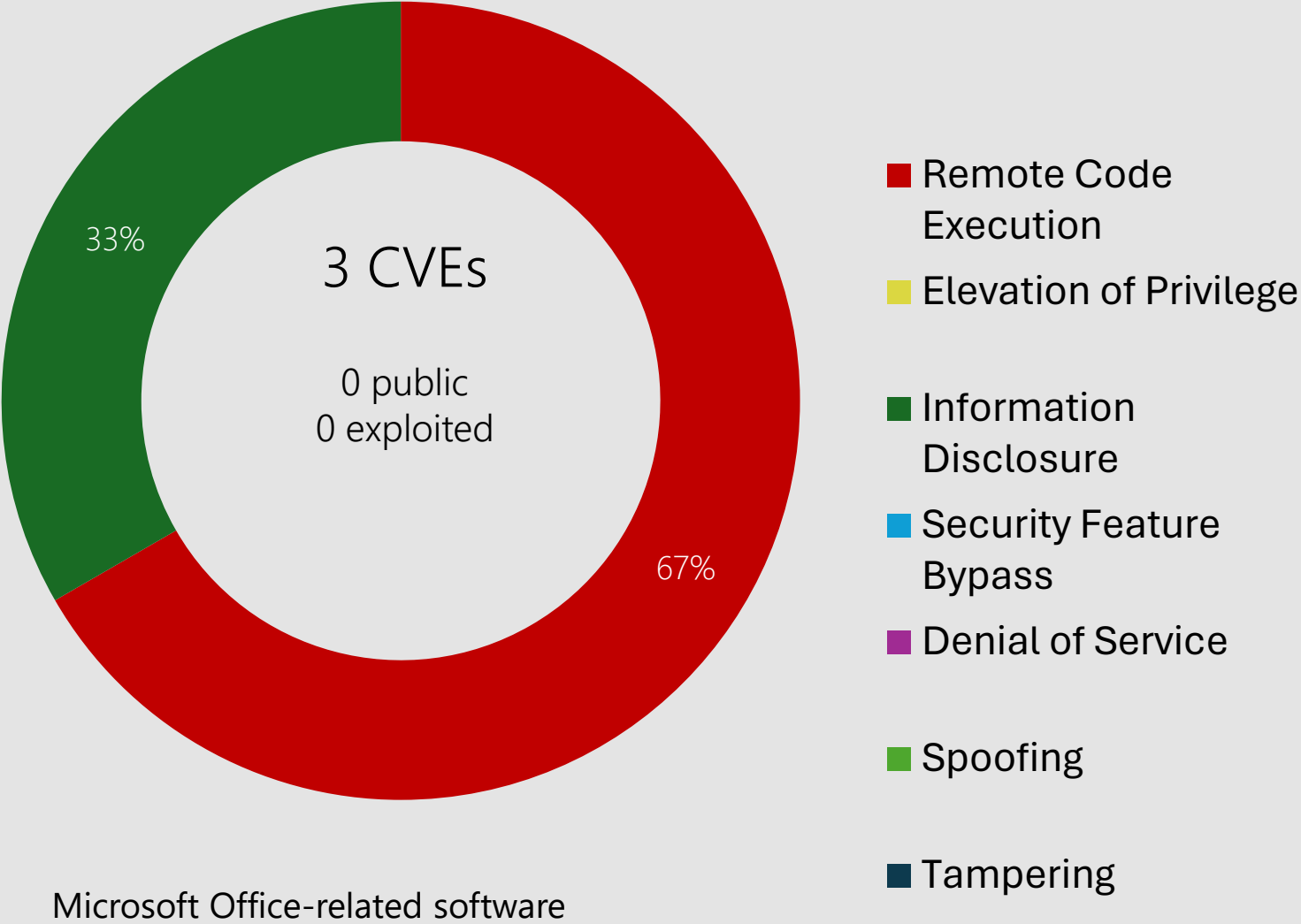
Microsoft has not identified any workarounds for this vulnerability.

# Affected Software



Windows 11  
Windows 10  
Server 2022  
Server 2019  
Server 2016

# Microsoft Office



## 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



## CVSS Score Metrics

Base CVSS Score: 8.8 | 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 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



## CVSS Score Metrics

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

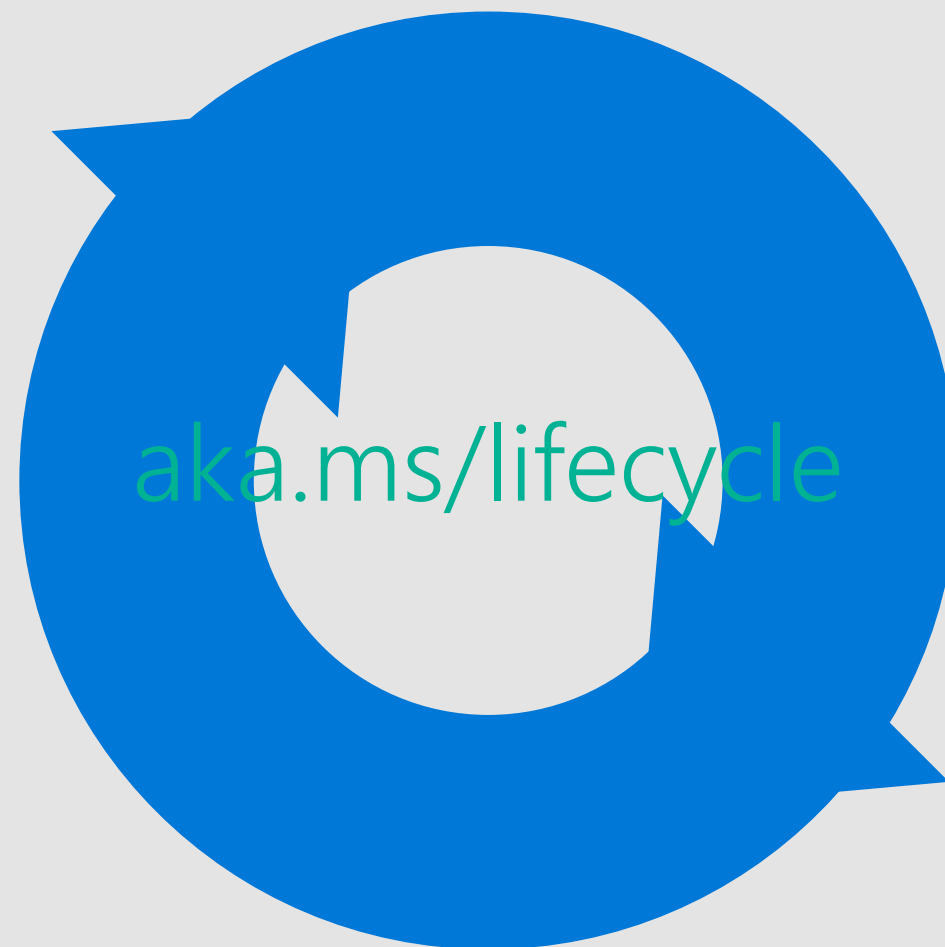
# Product Lifecycle Update

Modern Policy

Coming June 11, 2024

.NET 7

Windows 10 21H2 (Ent and EDU)



[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 

On this page 

 [Subscribe](#)  [RSS](#)  [PowerShell](#)  [API](#)

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



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

[illegible]

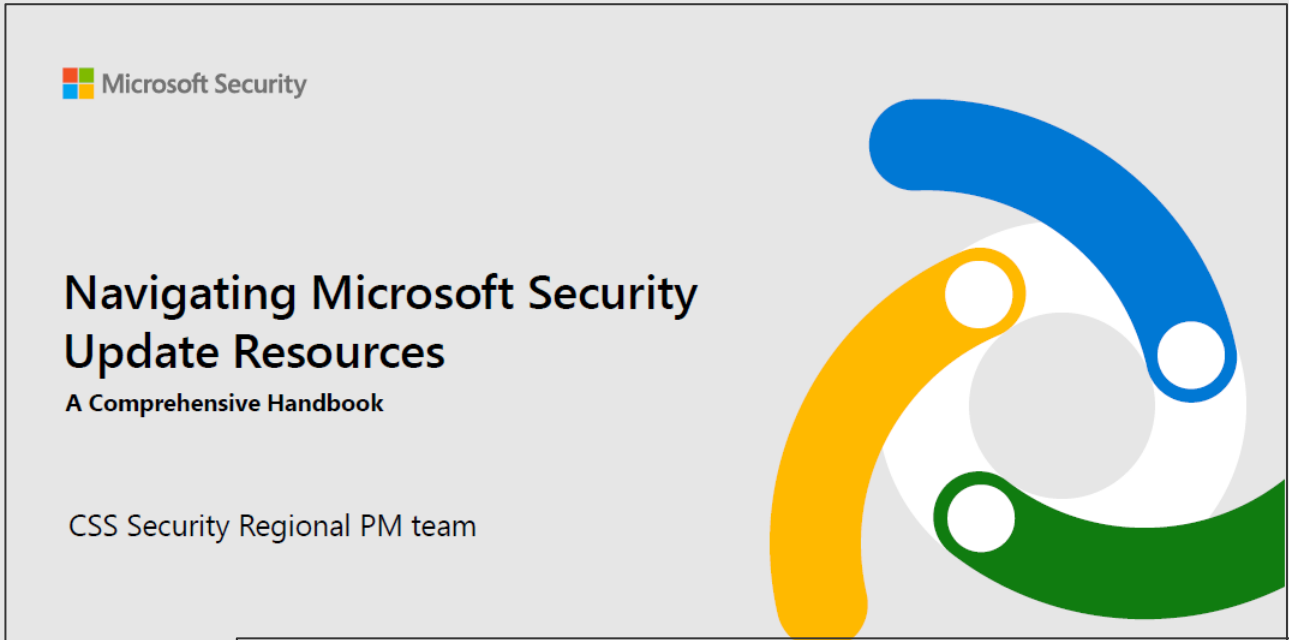
# Microsoft Monthly Security Briefing Extended Appendix

May 2024



# A Comprehensive Handbook for Microsoft Security Update Resources is now available

- Microsoft provides an array of valuable resources to manage security updates, yet many users remain unaware of their full potential.
- Our newly crafted Comprehensive Handbook “Microsoft Security Update Resources” aims to bridge this gap. This handbook provides a comprehensive guide on Microsoft Security Updates resources.
- Download: [Comprehensive Handbook Microsoft Security Update Resources](#)



Microsoft Security Vulnerabilities & Security Updates Publications				
Microsoft publishes security updates information at the following places.				
Who	Microsoft Security Response Center	Microsoft Update Windows Update	Product Groups	Microsoft Security
What	• Microsoft vulnerability information	• Update packages • Automatic updates delivery	• Product release notes • Update deployment guidance	• Detection and protection guidance • Vulnerability exploitation details
Where	• <a href="#">Security Update Guide – Microsoft</a> • <a href="#">Microsoft Security Response Center</a>	• <a href="#">Microsoft Update Catalog</a>	• Knowledge Base (KB) articles • Product team blogs	• <a href="#">Microsoft Security Blog</a>

# Summary of Security Updates released on Patch Tuesday

# Security Updates Overview

Product Family	Max Severity	Max. Impact	Security Update KB or Related resources
Windows 11 23H2 , v22H2, v21H2	Important	Remote Code Execution	v23H2, v22H2 <a href="#">5037771</a> v21H2 <a href="#">5037770</a>
Windows 10 v22H2, v21H2	Important	Remote Code Execution	<a href="#">5037768</a>
Windows Server 2022, 23H2 Edition (including Server Core installation)	Important	Remote Code Execution	Windows Server 2022, <a href="#">5037782</a> Hotpatch <a href="#">5037848</a> Windows Server 23H2, <a href="#">5036910</a>
Windows Server 2019 , 2016 (including Server Core installations)	Important	Remote Code Execution	Windows Server 2019, <a href="#">5037765</a> Windows Server 2016, <a href="#">5037763</a>
Microsoft Office	Important	Remote Code Execution	<a href="https://learn.microsoft.com/officeupdates">https://learn.microsoft.com/officeupdates</a>
Microsoft SharePoint	Critical	Remote Code Execution	<a href="https://learn.microsoft.com/officeupdates/sharepoint-updates">https://learn.microsoft.com/officeupdates/sharepoint-updates</a>
Microsoft .NET	Important	Remote Code Execution	<a href="https://learn.microsoft.com/dotnet">https://learn.microsoft.com/dotnet</a>
Microsoft Visual Studio	Important	Remote Code Execution	<a href="https://learn.microsoft.com/visualstudio">https://learn.microsoft.com/visualstudio</a>
Microsoft Dynamics 365	Important	Spoofing	<a href="https://learn.microsoft.com/dynamics365">https://learn.microsoft.com/dynamics365</a>
Microsoft Azure	Important	Spoofing	<a href="https://learn.microsoft.com/azure">https://learn.microsoft.com/azure</a>

# Security Vulnerability Overview

Product Family	Remote Code Execution	Elevation of Privilege	Information Disclosure	Security Feature Bypass	Denial of Service	Spoofing	Tampering	Publicly Disclosed	Known Exploit	Max CVSS
Windows 11 23H2 , v22H2 , v21H2	21	14	4	2	0	0	0	1	2	8.8
Windows 10 22H2 , 21H2	21	15	4	2	0	0	0	1	2	8.8
Windows Server 2022 Windows Server 23H2 Edition (Server Core installation)	22	15	5	2	2	0	0	1	2	8.8
Windows Server 2019	22	13	5	2	2	0	0	1	2	8.8
Windows Server 2016	11	10	4	2	2	0	0	1	2	8.8
Microsoft Office	1	0	0	0	0	0	0	0	0	7.8
Microsoft SharePoint	1	0	1	0	0	0	0	0	0	8.8
Microsoft .NET	1	0	0	0	0	0	0	0	0	6.3
Microsoft Visual Studio	2	0	0	0	1	0	0	1	0	8.1
Microsoft Dynamics 365	0	0	0	0	0	2	0	0	0	7.6
Microsoft Azure	0	0	0	0	0	1	0	0	0	6.5



# Publicly Disclosed/Exploited CVEs: Overview

CVE	Title	Max Severity	CVSS Base	Publicly Disclosed	Exploited
<a href="#">CVE-2024-30051</a>	Windows DWM Core Library Elevation of Privilege Vulnerability	Important	7.8	Yes	Yes
<a href="#">CVE-2024-30046</a>	Visual Studio Denial of Service Vulnerability	Important	5.9	Yes	No
<a href="#">CVE-2024-30040</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability	Important	8.8	No	Yes

# Re-released CVEs

CVE	Title	Revision Note	Released date Updated date
<a href="#">CVE-2024-28902</a> <a href="#">CVE-2024-26207</a> <a href="#">CVE-2024-26211</a> <a href="#">CVE-2024-26217</a> <a href="#">CVE-2024-28900</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability	CVE re-released to address a regression introduced in the April 2024 security updates. Customers affected by the regression should install the security updates released on May 14, 2024.	Released: Apr 9, 2024 Last updated: May 14, 2024
<a href="#">CVE-2024-23593</a>	Lenovo: CVE-2024-23593 Modify Boot Manager and Escalate Privileges	Updated CVE title and CVSS scores per request from CNA (Lenovo). This is an informational change only.	Released: Apr 9, 2024 Last updated: May 14, 2024

Enforcements / new features  
in this month' updates

# May 2024

- Retirement of RBAC Application Impersonation in Exchange Online

# Retirement of RBAC Application Impersonation in Exchange Online

We will begin blocking the assignment of the ApplicationImpersonation role in Exchange Online to accounts starting in **May 2024**, and that in February 2025, we will completely remove this role and its feature set from Exchange Online.

## How Does This Affect Me?:

All apps must have an App Registration, and when using Application permissions (not Delegated), the app must use a secure credential for access. When using EWS, grant scoped access using [RBAC for Apps](#). Better yet, use Graph, as [EWS is going away](#)!

## How Do I Find Accounts Using This Type of Access and What Actions Should I Take?:

Use [Exchange Online PowerShell](#) to check for accounts that have been assigned the ApplicationImpersonation role:  
> Get-ManagementRoleAssignment –Role ApplicationImpersonation –GetEffectiveUsers

For EWS applications requiring 1 to many mailbox access, ensure the application [is configured properly with OAuth](#) to use App-only access. Implement resource-scoped access using [Role Based Access Control for Applications](#) in Exchange Online to control mailbox access as needed for your scenario.

See more at : [Retirement of RBAC Application Impersonation in Exchange Online](#)

Newly announced or updated  
deprecations/enforcements/  
new features

# TLS server authentication: Deprecation of weak RSA certificates

TLS server authentication is becoming more secure across Windows. Weak RSA key lengths for certificates will be deprecated on future Windows OS releases later this year. Specifically, this affects TLS server authentication certificates chaining to roots in the Microsoft Trusted Root Program.

- Deprecation of weak RSA key lengths

TLS server authentication certificates are used to verify the identity of the server to a client and to establish secure connections between client and server. So far, you've been able to use 1024 bits as the shortest key length for RSA encryption. However, 1024-bit key lengths today provide insufficient security given the advancement of computing power and cryptanalysis techniques. Therefore, they will be discontinued in the last quarter of this calendar year.

Here's a timeline of the journey toward key lengths of 2048 bits or longer:

- 2012: Our first advisory encourages moving away from keys shorter than 1024 bits.
- 2013: The National Institute of Science and Technology (NIST) recommends discontinuing the use of 1024-bit RSA keys.
- 2016: You've been able to follow our Certification Authority Guidance to start implementing longer keys, among other measures.
- April 2024: The new recommended standard is available to those in the Windows Insider Program.
- **Late 2024:** 1024-bit RSA keys will be deprecated to further align with the latest internet standards and regulatory bodies.

In the coming months, Microsoft will begin to deprecate the use of TLS server authentication certificates using RSA key lengths shorter than 2048 bits on Windows Client. We recommend you use a stronger solution of at least 2048 bits length or an ECDSA certificate, if possible.

See more at : [TLS server authentication: Deprecation of weak RSA certificates](#)

# Reminder: Upcoming Updates/deprecations



# July 2024

- **Manager changes associated with CVE-2023-24932 [KB5025885](#) | Final Deployment Phase:** This phase is when we encourage customers to begin deploying the mitigations and managing any media updates. The updates will add the following changes:
  - Guidance and tooling to aid in updating media.
  - Updated DBX block to revoke additional boot managers.

# KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Summary

- On May 9 2023, Microsoft has released [CVE-2023-24932](#), and [associated configuration guidance](#), to address a Secure Boot bypass vulnerability used by the BlackLotus bootkit
- Firmware Interface (UEFI) through the Windows kernel Trusted Boot sequence. Secure Boot helps prevent bootkit malware in the boot sequence. Disabling Secure Boot puts a device at risk of being infected by bootkit malware. Fixing the Secure Boot bypass described in [CVE-2023-24932](#) requires revoking boot managers. This could cause issues for some device boot configurations.
- Mitigations against the Secure Boot bypass detailed in [CVE-2023-24932](#) are included in the Windows security updates that were released on or after April 9, 2024. However, these mitigations are not enabled by default. With these updates, we recommend that you begin evaluating these changes within your environment. The complete schedule is described in the [Timing of updates](#) section.
- Before you enable these mitigations, you should thoroughly review the details in this article and determine whether you have to enable the mitigations or wait for a future update from Microsoft. If you choose to enable the mitigations, you must verify your devices are updated and ready, and understand the risks described in this article ([KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 - Microsoft Support](#)).

# KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Enforcement Schedule

Date	Details
May 9, 2023 - Initial Deployment Phase	<p>In this release, to mitigate <a href="#">CVE-2023-24932</a>, the Windows Updates for May 9, 2023 include:</p> <ul style="list-style-type: none"><li>• Updates for Windows released on or after May 9, 2023 to address vulnerabilities discussed in <a href="#">CVE-2023-24932</a>.</li><li>• Changes to Windows boot components.</li><li>• Two revocation files which can be manually applied (a Code Integrity policy and an updated Secure Boot disallow list (DBX)).</li></ul>
July 11, 2023 - Second Deployment Phase	<p>Updates for Windows released on or after July 11, 2023 which adds the following:</p> <ul style="list-style-type: none"><li>• Allow easier, automated deployment of the revocation files (Code Integrity Boot policy and Secure Boot disallow list (DBX)).</li><li>• New Event Log events will be available to report whether revocation deployment was successful or not.</li><li>• SafeOS Dynamic Update package for Window Recovery Environment (WinRE).</li></ul>
April 9, 2024 or later - Evaluation Phase	<p>With this phase, we are asking that you test these changes in your environment to make sure that the changes work correctly with representative sample devices and to get experience with the changes.</p>
July 9, 2024 or later – Final Deployment Phase	<p>This phase is when we encourage customers to begin deploying the mitigations and managing any media updates. The updates will add the following changes:</p> <ul style="list-style-type: none"><li>• Guidance and tooling to aid in updating media.</li><li>• Updated DBX block to revoke additional boot managers.</li></ul>
Date to be announced – Enforcement Phase	<p>The Enforcement Phase will be at least six months after the Deployment Phase. When updates are released for the Enforcement Phase, they will include the following:</p> <p>The “Windows Production PCA 2011” certificate will automatically be revoked by being added to the Secure Boot UEFI Forbidden List (DBX) on capable devices. These updates will be programmatically enforced after installing updates for Windows to all affected systems with no option to be disabled.</p>

# KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Take Action

- The following steps should be followed:
- [Step 1: Install](#) the Windows security update released on or after April 9, 2024, on all supported versions.
- [Step 2: Evaluate](#) the changes and how they affect your environment.
- [Step 3: Enforce](#) the changes.

## More Information

- Read MSRC blog for overview: [Microsoft Security Response Center](#)
- Read [KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 - Microsoft Support](#) to learn about the phased deployment, additional actions necessary for complete protection, and potential impact
- Read [Revoking vulnerable Windows boot managers | Windows IT Pro blog \(microsoft.com\)](#)

## [Final Deployment Phase] KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

- This phase is when we encourage customers to begin deploying the mitigations and managing any media updates. The updates will add the following changes:
  - Guidance and tooling to aid in updating media.
  - Updated DBX block to revoke additional boot managers.

# October 2024

- [KB5037754](#): PAC Validation changes related to CVE-2024-26248 and CVE-2024-29056  
Enforced by Default Phase:
  - Updates released on or after October 15, 2024, will move all Windows domain controllers and clients in the environment to Enforced mode by changing the registry subkey settings to PacSignatureValidationLevel=3 and CrossDomainFilteringLevel=4, enforcing the secure behavior by default. The Enforced by Default settings can be overridden by an Administrator to revert to Compatibility mode.



# KB5037754: PAC Validation changes related to CVE-2024-26248 and CVE-2024-29056

## Summary

The Windows security updates released on or after April 9, 2024 address elevation of privilege vulnerabilities with the [Kerberos PAC Validation Protocol](#). The Privilege Attribute Certificate (PAC) is an extension to Kerberos service tickets. It contains information about the authenticating user and their privileges. This update fixes a vulnerability where the user of the process can spoof the signature to bypass PAC signature validation security checks added in [KB5020805: How to manage Kerberos protocol changes related to CVE-2022-37967](#).

To learn more about these vulnerabilities, visit [CVE-2024-26248](#) and [CVE-2024-29056](#).

## Take Action

IMPORTANT Step 1 to install the update released on or after April 9, 2024 will NOT fully address the security issues in [CVE-2024-26248](#) and [CVE-2024-29056](#) by default. To fully mitigate the security issue for all devices, you must move to Enforced mode (described in Step 3) once your environment is fully updated.

To help protect your environment and prevent outages, we recommend the following steps:

- 1.UPDATE: Windows domain controllers and Windows clients must be updated with a Windows security update released on or after April 9, 2024.
- 2.MONITOR: Audit events will be visible in Compatibility mode to identify devices not updated.
- 3.ENABLE: After Enforcement mode is fully enabled in your environment, the vulnerabilities described in [CVE-2024-26248](#) and [CVE-2024-29056](#) will be mitigated.

## Timeline of changes

Updates are released as follows. Note that this release schedule might be revised as needed.

**April 9, 2024: Initial Deployment Phase – Compatibility Mode:** The initial deployment phase starts with the updates released on April 9, 2024. This update adds new behavior that prevents the elevation of privilege vulnerabilities described in CVE-2024-26248 and CVE-2024-29056 but does not enforce it unless both Windows domain controllers and Windows clients in the environment are updated. To enable the new behavior and to mitigate the vulnerabilities, you must make sure your entire Windows environment (including both domain controllers and clients) is updated. Audit Events will be logged to help identify devices not updated.

**October 15, 2024: Enforced by Default Phase:** Updates released on or after October 15, 2024, will move all Windows domain controllers and clients in the environment to Enforced mode by changing the registry subkey settings to PacSignatureValidationLevel=3 and CrossDomainFilteringLevel=4, enforcing the secure behavior by default.

The Enforced by Default settings can be overridden by an Administrator to revert to Compatibility mode.

**April 8, 2025: Enforcement Phase:** The Windows security updates released on or after April 8, 2025, will remove support for the registry subkeys PacSignatureValidationLevel and CrossDomainFilteringLevel and enforce the new secure behavior. There will be no support for Compatibility mode after installing this update.

# November 2024

- TLS 1.0 and 1.1 support will be removed for new & existing Azure storage accounts starting



# TLS 1.0 and 1.1 support will be removed for new & existing Azure storage accounts starting Nov 1, 2024

[TLS 1.0 and 1.1 support will be removed for new & existing Azure storage accounts starting Nov 2024 - Microsoft Community Hub](#)

- To meet evolving technology and regulatory needs and align with security best practices, **we are removing support for Transport Layer Security (TLS) 1.0 and 1.1 for both existing and new storage accounts in all clouds. TLS 1.2 will be the minimum supported TLS version for Azure Storage starting Nov 1, 2024.**
- Azure Storage currently supports TLS 1.0 and 1.1 (for backward compatibility) and TLS 1.2 on public HTTPS endpoints. TLS 1.2 is more secure and faster than older TLS versions. TLS 1.0 and 1.1 do not support modern cryptographic algorithms and cipher suites. Many of the Azure storage customers are already using TLS 1.2 and we are sharing this guidance to expedite the transition for customers currently on TLS 1.0 and 1.1. Customers must secure their infrastructure by using TLS 1.2 with Azure Storage by Oct 31, 2024. The older TLS versions (1.0 and 1.1) are being deprecated and removed to meet evolving standards (FedRamp, NIST), and provide improved security for our customers.
- This change will impact both existing and new storage accounts using TLS 1.0 and 1.1. To avoid disruptions to your applications connecting to Azure Storage, you must migrate to TLS 1.2 and remove dependencies on TLS version 1.0 and 1.1, by Oct 31, 2024. Learn more about [how to migrate to TLS1.2](#).
- As best practice, we also recommend using Azure policy to enforce a minimum TLS version. Learn more [here](#) about how to enforce a minimum TLS version for all incoming requests. If you already use Azure Policy to enforce TLS version, minimum supported version after this change rolls out will be TLS 1.2.

# Late 2024

- [TLS server authentication: Deprecation of weak RSA certificates](#)
  - TLS server authentication is becoming more secure across Windows. Weak RSA key lengths for certificates will be deprecated on future Windows OS releases later this year. Specifically, this affects TLS server authentication certificates chaining to roots in the Microsoft Trusted Root Program.

# TLS server authentication: Deprecation of weak RSA certificates

TLS server authentication is becoming more secure across Windows. Weak RSA key lengths for certificates will be deprecated on future Windows OS releases later this year. Specifically, this affects TLS server authentication certificates chaining to roots in the Microsoft Trusted Root Program.

- Deprecation of weak RSA key lengths

TLS server authentication certificates are used to verify the identity of the server to a client and to establish secure connections between client and server. So far, you've been able to use 1024 bits as the shortest key length for RSA encryption. However, 1024-bit key lengths today provide insufficient security given the advancement of computing power and cryptanalysis techniques. Therefore, they will be discontinued in the last quarter of this calendar year.

Here's a timeline of the journey toward key lengths of 2048 bits or longer:

- 2012: Our first advisory encourages moving away from keys shorter than 1024 bits.
- 2013: The National Institute of Science and Technology (NIST) recommends discontinuing the use of 1024-bit RSA keys.
- 2016: You've been able to follow our Certification Authority Guidance to start implementing longer keys, among other measures.
- April 2024: The new recommended standard is available to those in the Windows Insider Program.
- **Late 2024:** 1024-bit RSA keys will be deprecated to further align with the latest internet standards and regulatory bodies.

In the coming months, Microsoft will begin to deprecate the use of TLS server authentication certificates using RSA key lengths shorter than 2048 bits on Windows Client. We recommend you use a stronger solution of at least 2048 bits length or an ECDSA certificate, if possible.

See more at : [TLS server authentication: Deprecation of weak RSA certificates](#)

# February 2025

- [KB5014754](#) Certificate-based authentication changes on Windows domain controllers (CVE-2022-34691, CVE-2022-26931 and CVE-2022-26923) | Final, full enforcement (Phase 3)
  - By February 11, 2025, all devices will be updated to Full Enforcement mode. In this mode, if a certificate fails the strong (secure) mapping criteria (see Certificate mappings), authentication will be denied.
- Retirement of RBAC Application Impersonation in Exchange Online
  - We will completely remove this role and its feature set from Exchange Online.

# KB5014754—Certificate-based authentication changes on Windows domain controllers Final, full enforcement

- Summary
  - [CVE-2022-34691](#), [CVE-2022-26931](#) and [CVE-2022-26923](#) address an elevation of privilege vulnerability that can occur when the Kerberos Key Distribution Center (KDC) is servicing a certificate-based authentication request. Before the May 10, 2022 security update, certificate-based authentication would not account for a dollar sign (\$) at the end of a machine name. This allowed related certificates to be emulated (spoofed) in various ways. Additionally, conflicts between User Principal Names (UPN) and sAMAccountName introduced other emulation (spoofing) vulnerabilities that we also address with this security update.
- Take action: To protect your environment, complete the following steps for certificate-based authentication:
  1. Update all servers that run Active Directory Certificate Services and Windows domain controllers that service certificate-based authentication with the May 10, 2022 update (see [Compatibility mode](#)). The May 10, 2022 update will provide [audit events](#) that identify certificates that are not compatible with Full Enforcement mode.
  2. If no audit event logs are created on domain controllers for one month after installing the update, proceed with enabling [Full Enforcement mode](#) on all domain controllers. By February 11, 2025, all devices will be updated to Full Enforcement mode. In this mode, if a certificate fails the strong (secure) mapping criteria (see [Certificate mappings](#)), authentication will be denied.
- Please review [KB5014754—Certificate-based authentication changes on Windows domain controllers - Microsoft Support](#) for more information.

# Retirement of RBAC Application Impersonation in Exchange Online

We will begin blocking the assignment of the ApplicationImpersonation role in Exchange Online to accounts starting in May 2024, and that in **February 2025**, we will completely remove this role and its feature set from Exchange Online.

## How Does This Affect Me?:

All apps must have an App Registration, and when using Application permissions (not Delegated), the app must use a secure credential for access. When using EWS, grant scoped access using [RBAC for Apps](#). Better yet, use Graph, as [EWS is going away](#)!

## How Do I Find Accounts Using This Type of Access and What Actions Should I Take?:

Use [Exchange Online PowerShell](#) to check for accounts that have been assigned the ApplicationImpersonation role:  
> Get-ManagementRoleAssignment –Role ApplicationImpersonation –GetEffectiveUsers

For EWS applications requiring 1 to many mailbox access, ensure the application [is configured properly with OAuth](#) to use App-only access. Implement resource-scoped access using [Role Based Access Control for Applications](#) in Exchange Online to control mailbox access as needed for your scenario.

See more at : [Retirement of RBAC Application Impersonation in Exchange Online](#)



# April 2025

- [KB5037754](#): PAC Validation changes related to CVE-2024-26248 and CVE-2024-29056  
**Enforcement Phase:** The Windows security updates released on or after April 8, 2025, will remove support for the registry subkeys PacSignatureValidationLevel and CrossDomainFilteringLevel and enforce the new secure behavior. There will be no support for Compatibility mode after installing this update.

# [KB5037754](#): PAC Validation changes related to CVE-2024-26248 and CVE-2024-29056

## Summary

The Windows security updates released on or after April 9, 2024 address elevation of privilege vulnerabilities with the [Kerberos PAC Validation Protocol](#). The Privilege Attribute Certificate (PAC) is an extension to Kerberos service tickets. It contains information about the authenticating user and their privileges. This update fixes a vulnerability where the user of the process can spoof the signature to bypass PAC signature validation security checks added in [KB5020805: How to manage Kerberos protocol changes related to CVE-2022-37967](#).

To learn more about these vulnerabilities, visit [CVE-2024-26248](#) and [CVE-2024-29056](#).

## Take Action

IMPORTANT Step 1 to install the update released on or after April 9, 2024 will NOT fully address the security issues in [CVE-2024-26248](#) and [CVE-2024-29056](#) by default. To fully mitigate the security issue for all devices, you must move to Enforced mode (described in Step 3) once your environment is fully updated.

To help protect your environment and prevent outages, we recommend the following steps:

- 1.UPDATE: Windows domain controllers and Windows clients must be updated with a Windows security update released on or after April 9, 2024.
- 2.MONITOR: Audit events will be visible in Compatibility mode to identify devices not updated.
- 3.ENABLE: After Enforcement mode is fully enabled in your environment, the vulnerabilities described in [CVE-2024-26248](#) and [CVE-2024-29056](#) will be mitigated.

## Timeline of changes

Updates are released as follows. Note that this release schedule might be revised as needed.

**April 9, 2024: Initial Deployment Phase – Compatibility Mode:** The initial deployment phase starts with the updates released on April 9, 2024. This update adds new behavior that prevents the elevation of privilege vulnerabilities described in CVE-2024-26248 and CVE-2024-29056 but does not enforce it unless both Windows domain controllers and Windows clients in the environment are updated. To enable the new behavior and to mitigate the vulnerabilities, you must make sure your entire Windows environment (including both domain controllers and clients) is updated. Audit Events will be logged to help identify devices not updated.

**October 15, 2024: Enforced by Default Phase:** Updates released on or after October 15, 2024, will move all Windows domain controllers and clients in the environment to Enforced mode by changing the registry subkey settings to PacSignatureValidationLevel=3 and CrossDomainFilteringLevel=4, enforcing the secure behavior by default.

The Enforced by Default settings can be overridden by an Administrator to revert to Compatibility mode.

**April 8, 2025: Enforcement Phase:** The Windows security updates released on or after April 8, 2025, will remove support for the registry subkeys PacSignatureValidationLevel and CrossDomainFilteringLevel and enforce the new secure behavior. There will be no support for Compatibility mode after installing this update.



# Date to be announced

- [KB5025885](#): How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 Date to be announced – Enforcement Phase

The Enforcement Phase will be at least six months after the Deployment Phase. When updates are released for the Enforcement Phase, they will include the following:

The “Windows Production PCA 2011” certificate will automatically be revoked by being added to the Secure Boot UEFI Forbidden List (DBX) on capable devices. These updates will be programmatically enforced after installing updates for Windows to all affected systems with no option to be disabled.

# [KB5025885](#): How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Summary

- On May 9 2023, Microsoft has released [CVE-2023-24932](#), and [associated configuration guidance](#), to address a Secure Boot bypass vulnerability used by the BlackLotus bootkit
- Firmware Interface (UEFI) through the Windows kernel Trusted Boot sequence. Secure Boot helps prevent bootkit malware in the boot sequence. Disabling Secure Boot puts a device at risk of being infected by bootkit malware. Fixing the Secure Boot bypass described in [CVE-2023-24932](#) requires revoking boot managers. This could cause issues for some device boot configurations.
- Mitigations against the Secure Boot bypass detailed in [CVE-2023-24932](#) are included in the Windows security updates that were released on or after April 9, 2024. However, these mitigations are not enabled by default. With these updates, we recommend that you begin evaluating these changes within your environment. The complete schedule is described in the [Timing of updates](#) section.
- Before you enable these mitigations, you should thoroughly review the details in this article and determine whether you have to enable the mitigations or wait for a future update from Microsoft. If you choose to enable the mitigations, you must verify your devices are updated and ready, and understand the risks described in this article ([KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 - Microsoft Support](#)).

# [KB5025885](#): How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Enforcement Schedule

Date	Details
May 9, 2023 - Initial Deployment Phase	<p>In this release, to mitigate <a href="#">CVE-2023-24932</a>, the Windows Updates for May 9, 2023 include:</p> <ul style="list-style-type: none"><li>• Updates for Windows released on or after May 9, 2023 to address vulnerabilities discussed in <a href="#">CVE-2023-24932</a>.</li><li>• Changes to Windows boot components.</li><li>• Two revocation files which can be manually applied (a Code Integrity policy and an updated Secure Boot disallow list (DBX)).</li></ul>
July 11, 2023 - Second Deployment Phase	<p>Updates for Windows released on or after July 11, 2023 which adds the following:</p> <ul style="list-style-type: none"><li>• Allow easier, automated deployment of the revocation files (Code Integrity Boot policy and Secure Boot disallow list (DBX)).</li><li>• New Event Log events will be available to report whether revocation deployment was successful or not.</li><li>• SafeOS Dynamic Update package for Window Recovery Environment (WinRE).</li></ul>
April 9, 2024 or later - Evaluation Phase	<p>With this phase, we are asking that you test these changes in your environment to make sure that the changes work correctly with representative sample devices and to get experience with the changes.</p>
July 9, 2024 or later – Final Deployment Phase	<p>This phase is when we encourage customers to begin deploying the mitigations and managing any media updates. The updates will add the following changes:</p> <ul style="list-style-type: none"><li>• Guidance and tooling to aid in updating media.</li><li>• Updated DBX block to revoke additional boot managers.</li></ul>
Date to be announced – Enforcement Phase	<p>The Enforcement Phase will be at least six months after the Deployment Phase. When updates are released for the Enforcement Phase, they will include the following:</p> <p>The “Windows Production PCA 2011” certificate will automatically be revoked by being added to the Secure Boot UEFI Forbidden List (DBX) on capable devices. These updates will be programmatically enforced after installing updates for Windows to all affected systems with no option to be disabled.</p>

# [KB5025885](#): How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

## Take Action

- The following steps should be followed:
- [Step 1: Install](#) the Windows security update released on or after April 9, 2024, on all supported versions.
- [Step 2: Evaluate](#) the changes and how they affect your environment.
- [Step 3: Enforce](#) the changes.

## More Information

- Read MSRC blog for overview: [Microsoft Security Response Center](#)
- Read [KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932 - Microsoft Support](#) to learn about the phased deployment, additional actions necessary for complete protection, and potential impact
- Read: [Revoking vulnerable Windows boot managers | Windows IT Pro blog \(microsoft.com\)](#)

[Final Deployment Phase] [KB5025885](#): How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932

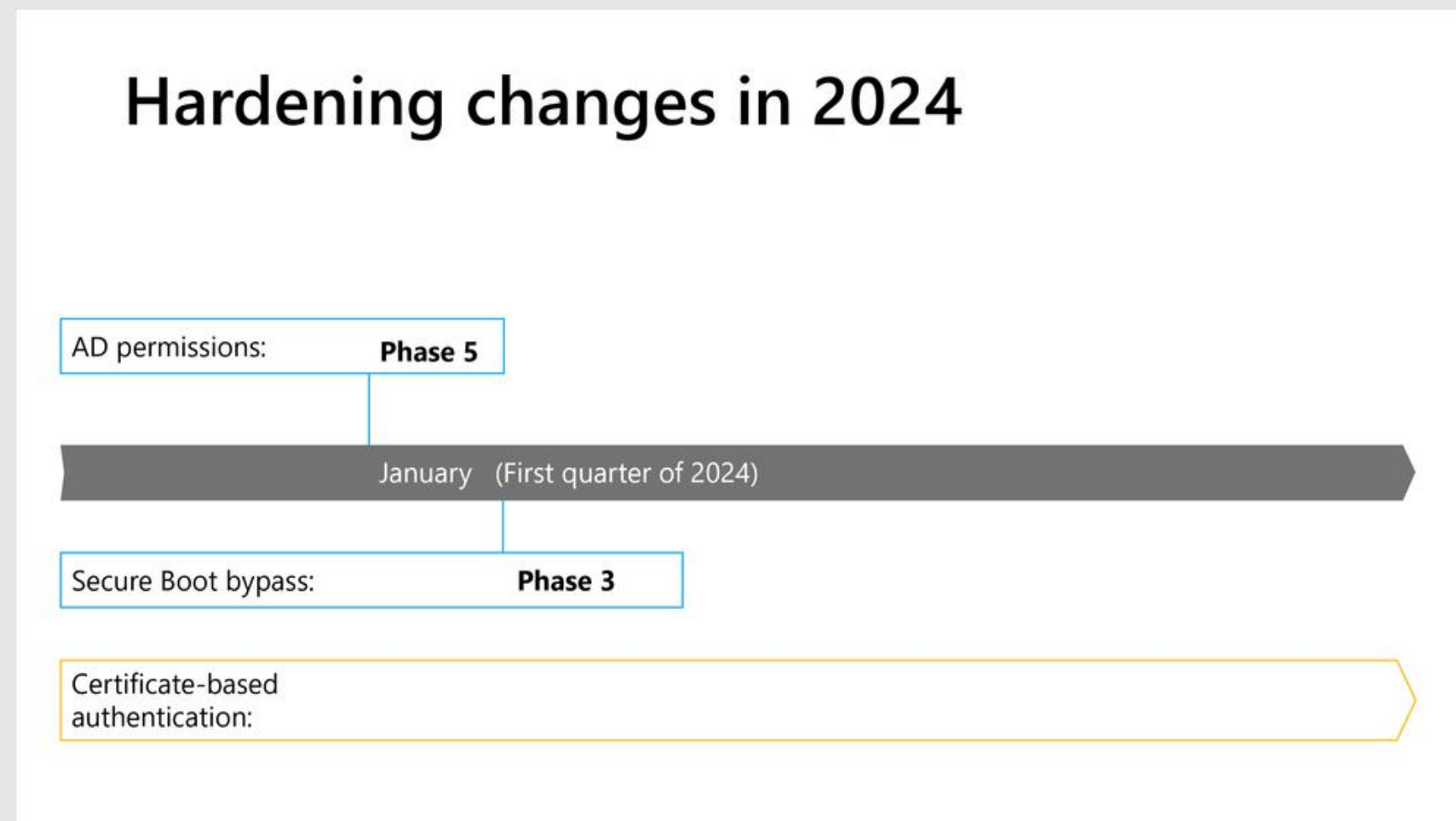
The Enforcement Phase will be at least six months after the Deployment Phase. When updates are released for the Enforcement Phase, they will include the following:

The “Windows Production PCA 2011” certificate will automatically be revoked by being added to the Secure Boot UEFI Forbidden List (DBX) on capable devices. These updates will be programmatically enforced after installing updates for Windows to all affected systems with no option to be disabled.

# Resources

# Latest Windows hardening guidance and key dates

- Please see the summary of Windows hardening guidance and key dates at: [Latest Windows hardening guidance and key dates - Microsoft Community Hub](#)
- Please bookmark the [Windows message center](#) to easily find the latest updates and reminders. And if you are an IT admin with access to the Microsoft 365 admin center, set up [Email preferences on the Microsoft 365 admin center](#) to receive important notifications and updates.
- Hardening changes at a glance: Review the visual timeline to focus on the specific changes that are of interest to you. Find the details for each phase below.



A visual timeline of the hardening changes taking place in 2024

# Resources: Important Changes (Deprecations)

- Power Apps and Power Automate:
  - [Important changes \(deprecations\) coming in Power Apps and Power Automate](#)
- Dynamics 365:
  - [Removed or deprecated platform features](#)
  - [Deprecated features in client, server, database](#)



# Recommended Resources for IT Admins

# Microsoft Security Blogs

# Microsoft Security Blogs

## [Toward greater transparency: Adopting the CWE standard for Microsoft CVEs](#)

*MSRC*

The MSRC (Microsoft Security Response Center) is now publishing root cause data for Microsoft CVEs using the [Common Weakness Enumeration \(CWE™\)](#) industry standard. The CWE is a community-developed list of common software and hardware weaknesses. Both industry and customers will benefit from greater transparency and interoperability through CWE adoption.

## [New Nested App Authentication for Office Add-ins: Legacy Exchange tokens off by default in October 2024](#)

*Microsoft 365 Platform*

Nested App Authentication (NAA) is now in public preview. NAA provides simpler authentication and top tier identity protection through APIs designed specifically for add-ins in Office hosts. In addition, legacy Exchange user identity tokens and callback tokens will be turned off by default for all Exchange Online tenants in October 2024.

## [Microsoft Defender for Cloud Adds Full Coverage for Azure Open-Source Relational Databases](#)

*Microsoft Defender for Cloud Blog*

Microsoft Defender for Cloud now provides full threat protection coverage for all instances of Azure open-source relational databases: PostgreSQL, MySQL and MariaDB.

## [Strategies to monitor and prevent vulnerable driver attacks](#)

*Microsoft Security Experts Blog*

The blog delves into the history of vulnerable driver attacks, explores effective hunting methodologies, and dissects strategies for prevention and monitoring.

## [Get end-to-end protection with Microsoft's unified security operations platform, now in public preview](#)

*Microsoft Security Blog*

Customers with a single Microsoft Sentinel workspace and at least one Defender XDR workload deployed can start enjoying the benefits of a unified experience in a production environment.

# Microsoft Security Blogs

## [Russian US election interference targets support for Ukraine after slow start](#)

*Microsoft on the Issues Blog*

The Microsoft Threat Intelligence Election Report reveals that foreign influence in the U.S. presidential election is primarily focused on undermining U.S. support for Ukraine by Russia, exploiting societal polarization by China, and combining cyber and influence operations by Iran.

## [Attackers exploiting new critical OpenMetadata vulnerabilities on Kubernetes clusters](#)

*Microsoft Security Blog*

Microsoft recently uncovered an attack that exploits new critical vulnerabilities in OpenMetadata to gain access to Kubernetes workloads and leverage them for cryptomining activity. The blog shares the analysis of the attack, provides guidance for identifying vulnerable clusters and using Microsoft security solutions like Microsoft Defender for Cloud to detect malicious activity, and shares indicators of compromise that defenders can use for hunting and investigation.

## [Recent advisories released](#)

*MSRC*

[ADV24202320 - Power Automate Defense in Depth Advisory](#) - When you install the Microsoft Power Automate application to a directory other than the default program files location, non-admin users may have write access to the PAD install folder. See the advisory for more detail and recommended steps.

[ADV24205871 - Microsoft MacOS Installer Defense in Depth Advisory](#) - An issue exists in some Microsoft MacOS Installers where an attacker may be able to gain elevation of privilege during the installation process of some products. See the advisory for more detail and recommended steps.

## [Defender support for CVE-2024-3400 affecting Palo Alto Networks firewalls](#)

*Microsoft Defender Vulnerability Management Blog*

On April 12, 2024, Palo Alto Networks released a security advisory on CVE-2024-3400, a critical vulnerability affecting several versions of PAN-OS, the operating system that runs on the company's firewalls. The Defender blog provides an Advanced Hunting query you can use with Defender Vulnerability Management to find a list of the potentially vulnerable devices.

# Microsoft Security Blogs

## [Register for the Graph API webinar on April 23](#)

*Windows Message Center*

Learn how you can use Graph API to access information on Windows known issues and product lifecycle in the [Graph API webinar](#).

## [Key end of support dates for Office 2016, 2019 Apps & Productivity Servers](#)

*Office End of Support Blog*

The blog provides a list of all the applications and servers (including Office 2016 and Office 2019) that will reach the end of support on October 14, 2025.

## [Exchange Online to retire Basic auth for Client Submission \(SMTP AUTH\)](#)

*Exchange Team Blog*

Exchange Online will permanently remove support for Basic authentication with Client Submission (SMTP AUTH) in September 2025. After this time, applications and devices will no longer be able to use Basic auth as an authentication method and must use OAuth when using SMTP AUTH to send email.

Related reading: [Exchange Online to introduce External Recipient Rate Limit](#)

## [Ingesting non-Microsoft cloud security data into Microsoft Sentinel for government & DIB customers](#)

*Microsoft Sentinel Blog*

The blog reviews the relationship between commercial and government cloud solutions as well as the compliance and architecture aspects of ingesting security data from non-Microsoft clouds into Sentinel.

Related reading: [Ingesting non-Microsoft cloud security data into Microsoft Sentinel for Gov & DIB customers part 2](#)

# Microsoft Security Blogs

## [New steps have been released to mitigate Kerberos signature validation vulnerabilities](#)

*Windows Message Center*

The April 2024 security update released on April 9, 2024 addresses a security vulnerability in the Kerberos PAC Validation Protocol. New **Take Action** steps have been released as part of [KB5037754](#) to prevent bypassing PAC signature validation security checks added in [KB5020805: How to manage Kerberos protocol changes related to CVE-2022-37967](#).

## [Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials](#)

*Microsoft Security Blog*

Microsoft Threat Intelligence assesses Forest Blizzard's objective in deploying GooseEgg is to gain elevated access to target systems and steal credentials and information. The blog provides technical information, patching, and steps users can take to defend themselves against attempts to exploit Print Spooler vulnerabilities on GooseEgg.

## [New Microsoft Incident Response guide helps simplify cyberthreat investigations](#)

*Microsoft Security Blog*

Microsoft Incident Response experts have created a [guide on using Windows Internals](#) for forensic investigations.

## [Expanding our Content Integrity tools to support global elections](#)

*Microsoft on the Issues Blog*

The blog announces the expansion of the private preview of Content Integrity tools to EU political parties and campaigns and news organizations from around the world.

## [5 ways a CNAPP can strengthen your multicloud security environment](#)

*Microsoft Security Blog*

The Microsoft guide [From plan to deployment: implementing a cloud-native application protection platform \(CNAPP\) strategy](#) (PDF) explores the aspects of the emergence of CNAPP (cloud-native application protection platform), what it can mean for your organization, and how to get started.

# Microsoft Security Blogs

## [Released: April 2024 Exchange Server Hotfix Updates](#)

*Exchange Team Blog*

Microsoft has released Hotfix Updates (HUs) that enable support for new functionality and address issues in the [March 2024 Security Update \(SU\)](#).

## [Securing millions of developers through 2FA](#)

*GitHub Blog*

Since the mandatory rollout of 2FA in March 2023, GitHub has seen an opt-in rate of nearly 95 percent across code contributors who received the 2FA requirement in 2023.

## [Revoking vulnerable Windows Boot managers](#)

*Windows IT Pro Blog*

Windows is making updates to address a known security vulnerability exploited by BlackLotus to bypass Windows Secure Boot. You now have the option to revoke trust of the Microsoft Windows Production PCA (Product Certificate Authority) 2011.

Related reading: [Reducing Windows 10, version 22H2 monthly LCU package size](#)

## [Embracing the Data Protection and Data Privacy Act: A strategic approach with Microsoft's Compliance](#)

*Security, Compliance, and Identity Blog*

Microsoft Compliance Manager is a comprehensive solution for organizations, designed to streamline the journey towards compliance with the Data Protection and Data Privacy (DPDP) Act 2023.

## [Microsoft Security Exposure Management introduces: Critical asset protection](#)

*Security, Compliance, and Identity Blog*

Microsoft Security Exposure Management is a solution for identifying and managing critical assets to mitigate risks associated with the expanding enterprise attack surface.

Related reading: [Operationalizing attack path insights](#)

# Microsoft Security Blogs

## [Trusted Signing is in public preview](#)

*Security, Compliance, and Identity Blog*

Trusted Signing is now in public preview. Trusted Signing service (formerly Azure Code Signing) is a Microsoft fully managed end-to-end signing solution for developers.

## [Expanding privacy protection in Microsoft Defender for individuals](#)

*Security, Compliance, and Identity Blog*

Privacy protection has been added to iOS in the U.S. and United Kingdom. Current privacy protection is being extended on Android to the United Kingdom. Privacy protection is coming soon to Windows and macOS and will be available in more regions in the coming months.

## [Microsoft Intune Remote Help adds full control for Mac](#)

*Microsoft Intune Blog*

Microsoft Intune Remote Help's capabilities now include full control support for macOS devices. IT help desks can view Mac devices and also take full control of them.



# Microsoft Security Blogs

[‘Dirty stream’ attack: Discovering and mitigating a common vulnerability pattern in Android apps](#)

*Microsoft Security Blog*

Microsoft discovered a path traversal-affiliated vulnerability pattern in multiple popular Android applications that could enable a malicious application to overwrite files in the vulnerable application’s home directory. Several vulnerable applications in the Google Play Store represented more than 4 billion installations.

[Public preview: External authentication methods in Microsoft Entra ID](#)

*Microsoft Entra Blog*

The public preview of external authentication methods in Microsoft Entra ID is scheduled for release in the first half of May 2024. This feature will allow you to use your preferred multifactor authentication (MFA) solution with Entra ID.

More from Entra: [Microsoft Entra announcements and demos at RSAC 2024](#), [Public preview: Expanding passkey support in Microsoft Entra ID](#)

[Critical asset protection with Microsoft Security Exposure Management](#)

*Security, Compliance, and Identity Blog*

The article discusses the challenges security teams face due to the expanding enterprise attack surface and introduces Microsoft Security Exposure Management as a solution for identifying and managing critical assets to mitigate risks effectively.

[VPN connections might fail after installing the April 2024 security update](#)

*Windows release health*

Windows devices might face VPN connection failures after installing the April 2024 security update ([KB5036893](#)) or the April 2024 non-security preview update.

# Microsoft Security Blogs

## [Examining the deception infrastructure in place behind code.microsoft.com](#)

*Microsoft Sentinel Blog*

The article details Microsoft's strategic use of the code.microsoft.com domain as a honeypot to gather threat intelligence, highlighting its evolution, successes, and eventual retirement due to increased public awareness.

## [What's new in Microsoft Intune: April 2024](#)

*Microsoft Intune Blog*

Microsoft Intune's new capabilities for cloud-native management include updated app supersedence for Win32 apps, remote diagnostics for Microsoft 365 apps on mobile devices, and a new Windows update distribution report for better visibility into the status of monthly quality updates on managed Windows devices.

## [CodeQL zero to hero part 3: Security research with CodeQL](#)

*GitHub Blog*

The blog provides an in-depth guide on using CodeQL for security research, offering practical challenges and insights into variant analysis, taint tracking queries, and techniques to enhance security workflows.

## [Offline Security Intelligence Update is now GA!!](#)

*Windows Defender for Endpoint*

Offline Security Intelligence Update is now generally available, enabling organizations to update security intelligence on Linux endpoints with limited internet access using a local hosting server, enhancing control over signature deployment on critical servers.

# Microsoft Security Blogs

## [Security above all else—expanding Microsoft’s Secure Future Initiative](#)

*Microsoft Security Blog*

Charlie Bell speaks to the expansion of SFI and commitment to making security a top priority at Microsoft, guided by the security principles of secure by design, secure by default, and secure operations.

## [Vulnerability assessment with Defender for servers, powered by Defender Vulnerability Management](#)

*Microsoft Defender for Cloud Blog*

Starting May 1, 2024, Microsoft is introducing unified vulnerability assessment; Defender for Cloud will now exclusively offer Microsoft Defender Vulnerability Management as its primary scanner across servers and containers.

## [Exchange Server roadmap update](#)

*Exchange Team Blog*

The blog provides a roadmap for upcoming Exchange Server milestones.

## [Building securely: Microsoft Build 2024](#)

*Security, Compliance, and Identity Blog*

Check out the [session catalog](#) to start building your own itinerary and maximize your Microsoft Build 2024 attendee experience.

## [Defender for Cloud Apps delivers new in-browser protection capabilities via Microsoft Edge](#)

*Microsoft Defender XDR Blog*

Microsoft Defender for Cloud Apps now provides new in-browser protection capabilities via Microsoft Edge to enable security teams to seamlessly manage how a user can interact with in-app data based on their risk profile.

# Microsoft Security Blogs

## [Enhanced response action experience from Threat Explorer](#)

*Microsoft Defender for Office 365 Blog*

The new Take action feature in the Email Entity and Email Summary panel that lets you take multiple actions at once from a single wizard is now available in [Threat explorer](#).

## [The Microsoft Threat Intelligence podcast](#)

*Microsoft Threat Intelligence on X*

In this episode of The Microsoft Threat Intelligence podcast, [@AndresFreundTec](#), Senior security researcher [@fr0gger](#), and [@sherrod\\_im](#) discuss the discovery of the XZ backdoor, as well as findings in tracking its development and the actor behind it.

## [TLS server authentication: Deprecation of weak RSA certificates](#)

*Windows IT Pro Blog*

Weak RSA key lengths for certificates will be deprecated on future Windows OS releases later this year. Specifically, this affects TLS server authentication certificates chaining to roots in the Microsoft Trusted Root Program.

## [New developments in Microsoft Entra ID Protection](#)

*Microsoft Entra Blog*

The latest developments in Entra ID Protection help you reduce the risks of token replay attacks by making it easier to deploy risk policies, understand their impact, and protect your organization from emerging threats.

## [RSA news: What's new in Defender XDR?](#)

*Microsoft Defender XDR Blog*

The following capabilities are now available in Microsoft Defender XDR:

AI-powered disruption of SaaS attacks

Native support for data security and operational technology (OT)

End to end protection in the unified security operations platform

# Microsoft Security Blogs

## [Security, Compliance, and Identity Blog](#)

Several SCI articles were published May 6, 2024:

[Respond to trending threats and adopt zero-trust with Exposure Management](#)

[Empower multiple teams and prioritize investigations with Insider Risk Management](#)

[Maximize data protection & minimize business disruption with Microsoft Purview Data Loss Prevention](#)

[A new era in data security with dynamic controls to manage data access and mitigate risks](#)

[Protect your data and recover from insider data sabotage](#)

## [Microsoft Defender for Cloud extends support to enable increased API security testing visibility](#)

*Microsoft Defender for Cloud Blog*

Customers can now choose from a variety of API security testing solutions in the Azure Marketplace and integrate the solutions within their DevOps pipelines, allowing security teams to have centralized visibility of the assessed API security posture within Defender for Cloud.

Related reading: [End to end container security with unified SOC experience, Microsoft Defender Experts Services Expanded Coverage Upcoming Preview](#)

## [NTLM traffic issue after installing the April 2024 security update](#)

*Windows release health – known issue*

May 3, 2024 - [KB5036909](#): After installing the April 2024 security update (KB5036909) on domain controllers (DCs), you might notice a significant increase in NTLM authentication traffic. Please see <https://aka.ms/wrh> for additional documentation on this known issue.

## [VPN connections might fail after installing the April 2024 security update](#)

*Windows release health – known issue*

April 30, 2024 - [KB5036893](#): Windows devices might face VPN connection failures after installing the April 2024 security update (KB5036893) or the April 2024 non-security preview update. Please see <https://aka.ms/wrh> for additional documentation on this known issue.

# Microsoft Tech Community Blogs

- Azure Network Security Blog [Microsoft announces new collaboration with MazeBolt RADAR™ DDoS testing](#)
- FastTrack for Azure [Azure Monitoring Packs - V2 is out!](#)
- FastTrack for Azure [The Ultimate Guide to Deciphering Azure Agents + Defender for Servers: Part 2](#)
- FastTrack for Azure [The Ultimate Guide to Deciphering Azure Agents + Defender for Servers: Part 3](#)
- Microsoft Mechanics Blog [Extend your data security to Microsoft Fabric](#)
- Microsoft Mechanics Blog [Is Azure the right place to run Red Hat Enterprise Linux workloads?](#)
- Apps on Azure Blog [Protecting your IP in the Azure Marketplace](#)
- Ask the Directory Services Team [NTLM vs Kerberos](#)
- Configuration Manager Blog [Update 2403 for Microsoft Configuration Manager current branch is now available.](#)
- Intune Customer Success [Enhancing admin capabilities with Microsoft Intune's remote Microsoft 365 application diagnostics](#)
- IIS Support Blog [Windows Server 2022 IIS web site TLS 1.3 does not work with client certificate authentication](#)
- Microsoft Defender for Cloud Blog [Microsoft Defender for Open-Source Relational Databases Now Supports Multicloud \(AWS RDS\)](#)
- Microsoft Defender for Cloud Blog [Protecting Containers: A Primer for Moving from an EDR-based Threat Approach](#)
- Microsoft Defender for IoT Blog [Introducing Single Sign-On \(SSO\) for Sensor Console: Enhanced Security and Streamlined Access](#)
- Microsoft Defender for Office 365 Blog [Attack Simulation Training is now available for GCC High and DoD customers](#)
- Microsoft Defender XDR Blog [Introducing the new Defender for Identity Health Alert API](#)
- Networking Blog [Announcing Zero Trust DNS Private Preview](#)
- Security, Compliance, and Identity Blog [Microsoft named an overall leader in KuppingerCole Leadership Compass for ITDR](#)

# Other

- See [Azure Status](#) for real-time updates on the status of Azure products and services by region.
- See [Microsoft 365 Service health status](#) or [@MSFT365Status](#) for real-time updates on service issues preventing tenant administrators from accessing Service health in the Microsoft 365 admin center.
- See [Azure Databases](#) for Azure tech community discussions.

# Additional Resources







# Security Update Guide (<https://aka.ms/SUG>)


## Create your profile and sign up for the new notifications




[Security Update Guide Notification System News: Create your profile now – Microsoft Security Response Center](#)

- Notifications are sent when information is added or changed in the Security Update Guide. You can sign up for the new notification system today so that when we reach Phase Two, you will receive them at the email address of your choice. Just like existing notification system, there are two types of notifications – major updates and all updates. Major updates include new CVEs that are published and existing CVEs that are republished due to a change in software updates in the Security Updates table. Major updates, or Revisions, are marked with an incremented initial number such as 1.0, 2.0, etc. Minor updates are changes to FAQs or Acknowledgements or other informational type revisions. These types of revisions are marked with an incremented final number such as 1.1, 3.2, etc.

 **Microsoft** | **MSRC** | [Security Updates](#) | [Acknowledgements](#) | [Developer](#)

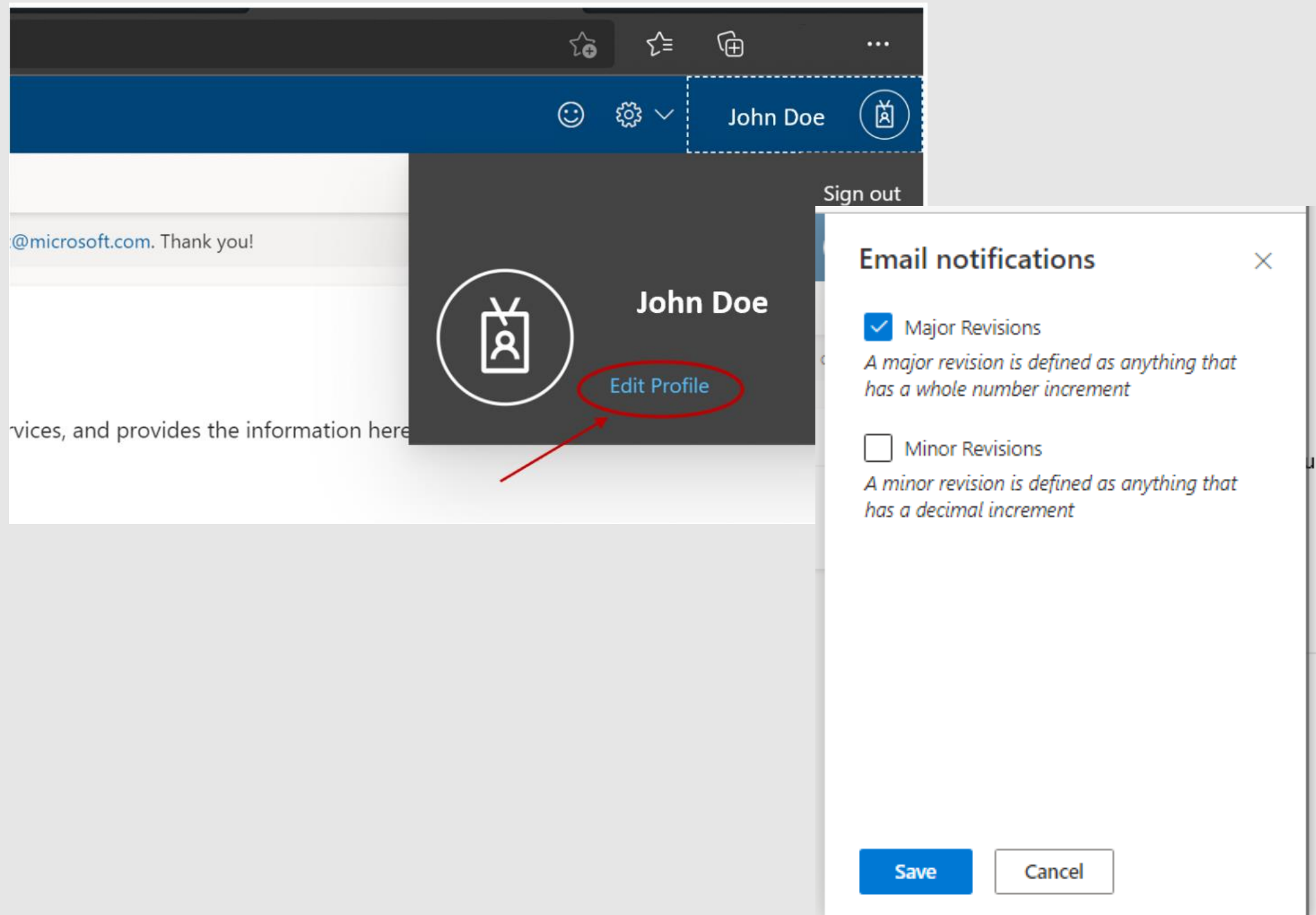
   Sign in

 **Looking for email notifications?** Please create your profile with your preferred email address to sign up for notifications. [See our blog post for more information](#).

 [Go to profile to subscribe](#)  [Hide for now](#)  [Don't show again](#)

# Steps to sign up for notifications

- To sign up for notifications, click the **Profile** and sign in. You will know you have successfully signed in when your Profile name is displayed.
- To opt into notifications, click on your Profile name and then select **Edit Profile** in the pop-up menu.
- Click **Edit** on the Email notifications column to select the type of notifications you would like to receive.
- In the panel that is displayed on the right-hand side, select the types of notifications you want to receive. If you select **Major Revisions**, you will receive only notifications for major updates. If you select **Minor Revisions**, you will receive all notifications for both major and minor updates. Click **Save** when you're finished.
- Click **Edit** on the Email notifications column to select the type of notifications you would like to receive.
- In the panel that is displayed on the right-hand side, select the types of notifications you want to receive. If you select **Major Revisions**, you will receive only notifications for major updates. If you select **Minor Revisions**, you will receive all notifications for both major and minor updates. Click **Save** when you're finished.



# Microsoft Monthly Security Briefing

Available for Unified Support customers

The Microsoft Security Response Center (MSRC) releases security updates on a monthly basis that address security vulnerabilities in Microsoft software, describe their remediation, and provide links to the applicable updates for affected software. This Security Briefing will provide concise, actionable information for IT professionals and security decision makers about the month's release. The session, hosted by Microsoft security subject matter experts, starts with a brief technical overview of the latest security bulletins and related content. The remainder of the session is dedicated to customer questions or concerns in an interactive, question-and-answer format.

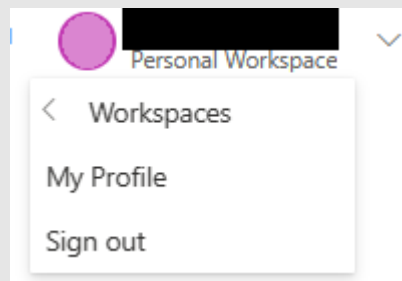
- **Presenter:** Security team, Customer Services and Support
- **Target Audience:** This Security Briefing is targeting Chief Information Security Officers, Security Vulnerability Assessors, IT Admins, and other security software update deployment decision makers
- **Key Features and Benefits:**
  - Learn about this month's security bulletin release.
  - Consolidated information - security update information is typically scattered in a variety of sources (TechNet, blogs, KB articles). This offering provides a cohesive view of the month's release.
  - Get your questions about the security bulletins and advisories answered.
  - Get current on product lifecycle information.

# Microsoft Monthly Security Briefing

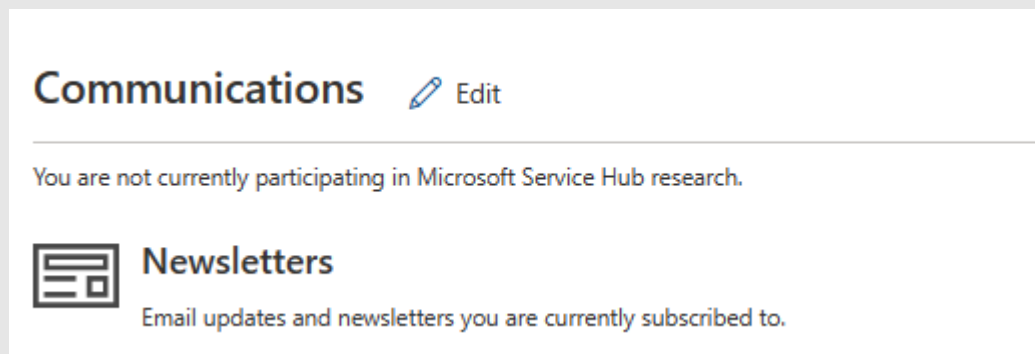
Available for Unified Support customers

How to subscribe invitation for Microsoft Monthly Security Briefing:

1. Sign in to [Services Hub](#)
2. Navigate to Upper right hand corner and click your account name and click [My Profile]



3. Navigate to [Communications] and click [Edit]



# Microsoft Monthly Security Briefing

Available for Unified Support customers

How to subscribe invitation for Microsoft Monthly Security Briefing (Continued):

4. Click [Filters] and type “Security Briefing” in [Name]

5. Change [Subscribed] to [Yes] for the security briefing call in your region/language.

Communications

Set your preferences for Services Hub email updates and newsletters

☐

I want to participate in Microsoft Enterprise Support research. I agree to these terms and conditions. [Terms & Conditions](#)

☒

I would like information, tips, and offers about Microsoft Enterprise Support, including the Services Hub. [Privacy Statement](#)

Newsletters

Select the toggle for newsletters you want to receive and save your choices.

Customer: Contoso Company

Subscription changes will be applied to: yurikam@microsoft.com

Newsletters Count (8)

✕ Clear Filters

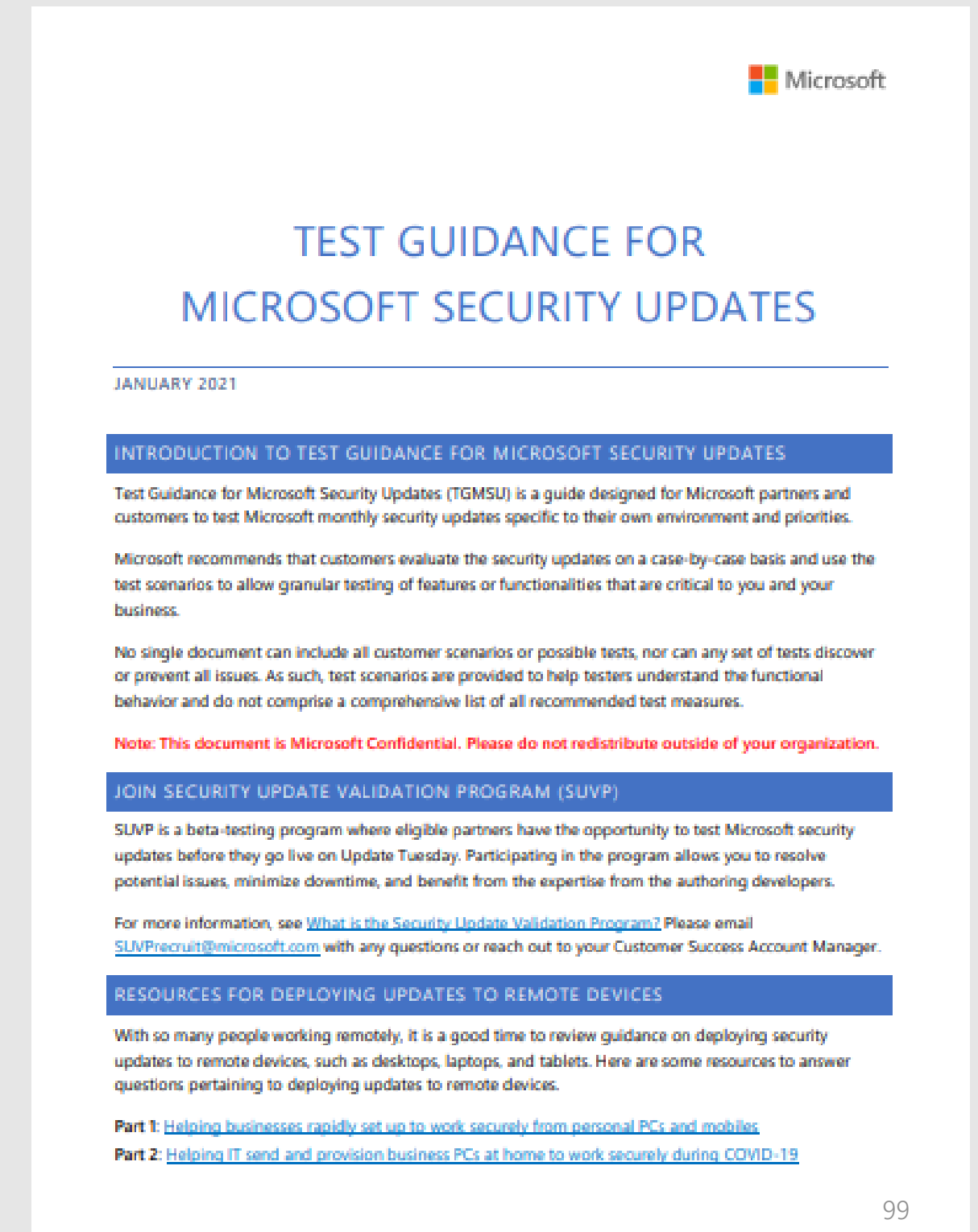
🔼 Hide Filters



# Test Guidance for Microsoft Security Updates (TGMSU)

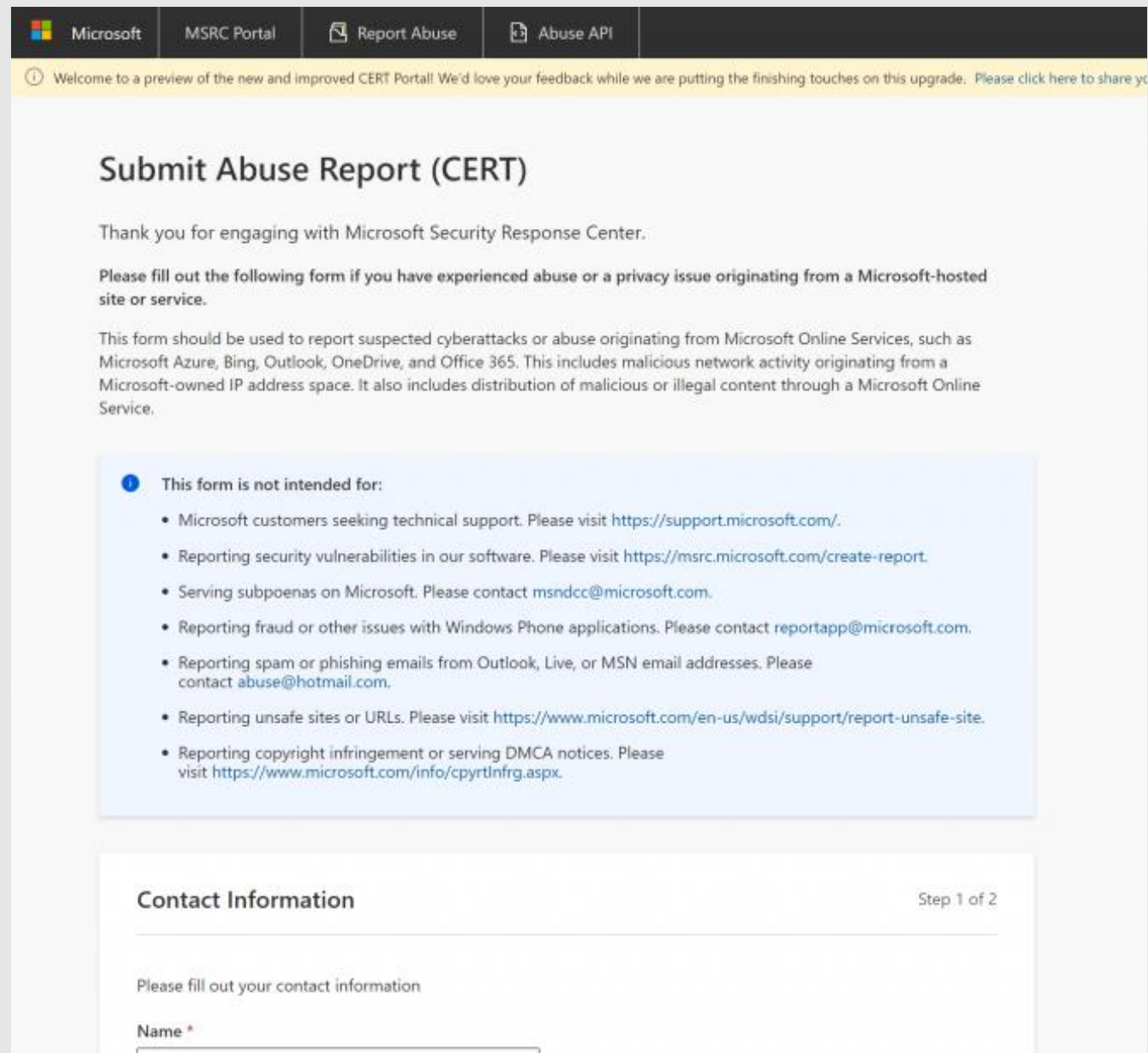
## Available for Unified Support customers

- Test Guidance for Microsoft Security Updates (TGMSU) is a guide designed for Microsoft partners and customers to test Microsoft monthly security updates specific to their own environment and priorities.
- Microsoft recommends that customers evaluate the security updates on a case-by-case basis and use the test scenarios to allow granular testing of features or functionalities that are critical to you and your business.
- No single document can include all customer scenarios or possible tests, nor can any set of tests discover or prevent all issues. As such, test scenarios are provided to help testers understand the functional behavior and do not comprise a comprehensive list of all recommended test measures.



# Report Abuse Portal and API

New Portal: <https://msrc.microsoft.com/report/abuse>



Microsoft MSRC Portal Report Abuse Abuse API

Welcome to a preview of the new and improved CERT Portal! We'd love your feedback while we are putting the finishing touches on this upgrade. Please click here to share your feedback.

## Submit Abuse Report (CERT)

Thank you for engaging with Microsoft Security Response Center.

Please fill out the following form if you have experienced abuse or a privacy issue originating from a Microsoft-hosted site or service.

This form should be used to report suspected cyberattacks or abuse originating from Microsoft Online Services, such as Microsoft Azure, Bing, Outlook, OneDrive, and Office 365. This includes malicious network activity originating from a Microsoft-owned IP address space. It also includes distribution of malicious or illegal content through a Microsoft Online Service.

**This form is not intended for:**

- Microsoft customers seeking technical support. Please visit <https://support.microsoft.com/>.
- Reporting security vulnerabilities in our software. Please visit <https://msrc.microsoft.com/create-report>.
- Serving subpoenas on Microsoft. Please contact [msndcc@microsoft.com](mailto:msndcc@microsoft.com).
- Reporting fraud or other issues with Windows Phone applications. Please contact [reportapp@microsoft.com](mailto:reportapp@microsoft.com).
- Reporting spam or phishing emails from Outlook, Live, or MSN email addresses. Please contact [abuse@hotmail.com](mailto:abuse@hotmail.com).
- Reporting unsafe sites or URLs. Please visit <https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site>.
- Reporting copyright infringement or serving DMCA notices. Please visit <https://www.microsoft.com/info/cpyrtlnfrg.aspx>.

### Contact Information

Step 1 of 2

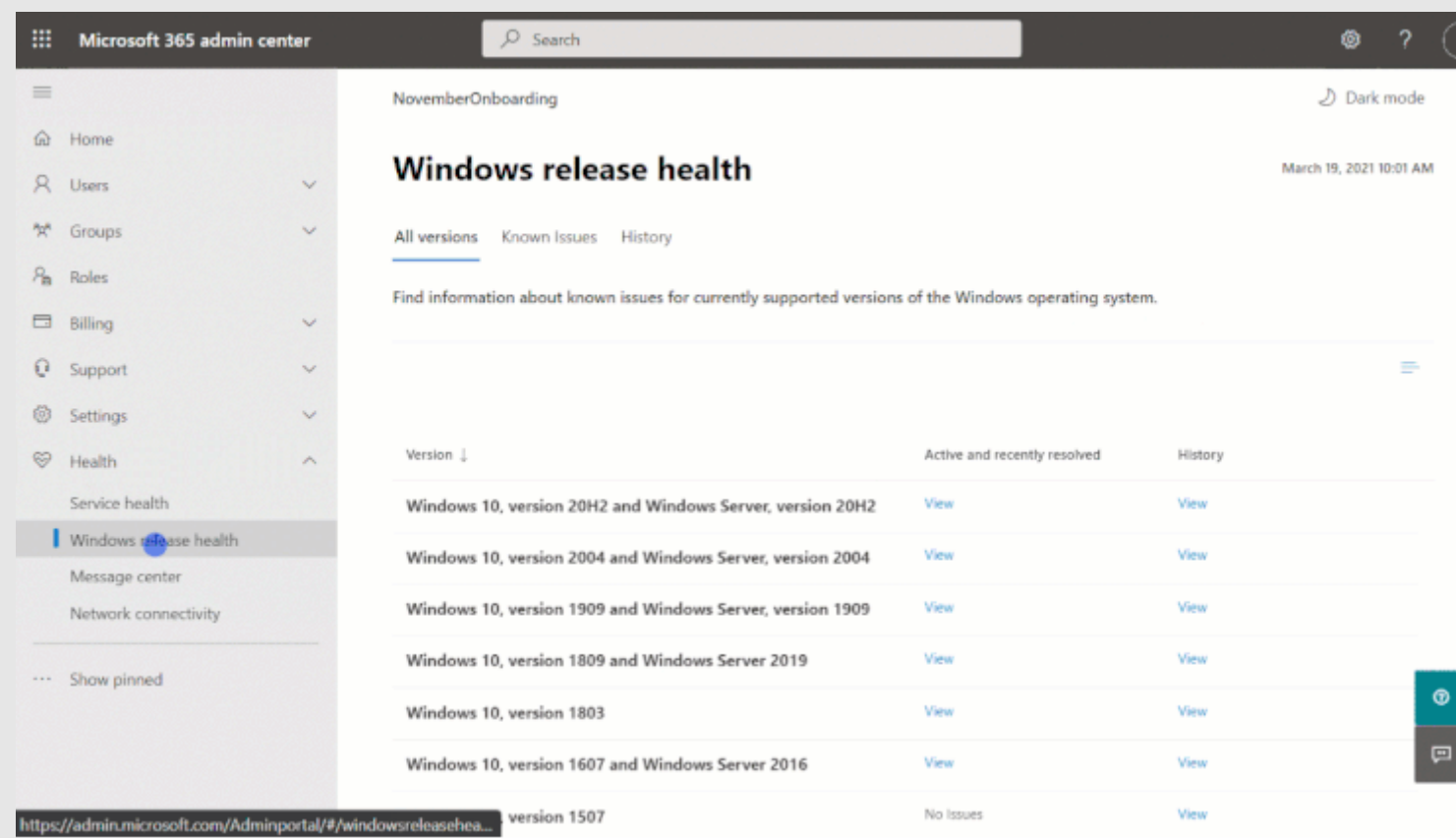
Please fill out your contact information

Name \*

- The [Report Abuse \(CERT\) Portal](#) and [Report Abuse API](#) have played a significant role in MSRC's response to suspected cyberattacks, privacy issues, and abuse originating from Microsoft Online Services.
- We have updated our Report Abuse Portal and API to include more granular and up-to-date reportable security incidents, empowering our community to provide more accurate and relevant insights.
  - [List of reportable security incidents](#)
- Read more at <https://msrc-blog.microsoft.com/2021/02/01/new-and-improved-report-abuse-portal-and-api/>

# Windows release health in the admin center

- Windows and Microsoft 365 IT admins now have easy, integrated access to essential information about monthly quality and feature updates, the latest features and enhancements for IT, servicing milestones, and lifecycle updates.
- The Windows release health experience on the admin center also offers insights into known issues, workarounds, and resolutions related to Windows updates.



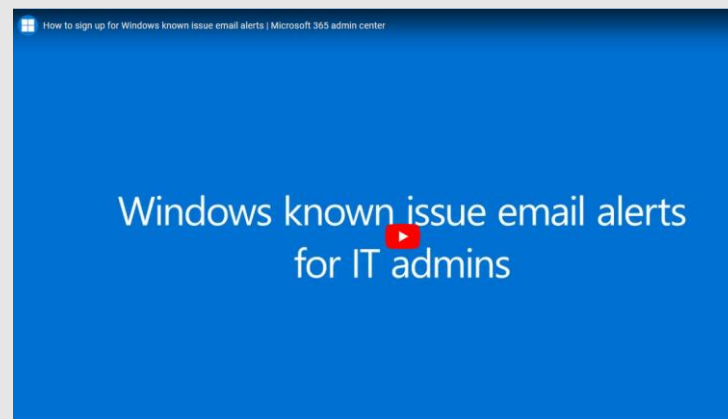
- visit <https://admin.microsoft.com>, log in, and scroll down to **Health** in the navigation menu. **Windows release health** will be listed underneath the existing **Service health** menu option.
- In order to access Windows release health in the admin center, you will need an applicable Microsoft 365<sup>[1]</sup> or Windows<sup>[2]</sup> licensing subscription, and to have the role of Service support admin for your tenant.

- Read more at [How to check Windows release health - Windows Deployment | Microsoft Docs](#)



# New feature: Sign up for Windows known issue email alerts

- You can get notified about Windows known issues documented in the [Windows release health](#) section of the Microsoft 365 admin center.
- This enables you to easily and quickly learn about issues related to Windows updates and make informed decisions about rolling out an update across your environment.
- When you sign up, you'll receive emails about new issues for the versions of the Windows operating system you support, as well as updates to known issues such as:
  - Changes in issue status
  - New workarounds
  - Issue resolution
- This new feature is available to IT admins with a Windows or Microsoft 365 tenant, a subscription that provides access to Windows release health in the Microsoft 365 admin center<sup>[1]</sup>, and an eligible admin role.
- Read more at: <https://aka.ms/WRH/NotifyMe>



Watch this short video for a quick step-by-step on how to set up email notifications for Windows known issues.

<https://yQSD7fYyodC4outu.be/>

# New CVE Communication Process for Azure vulnerabilities

- Microsoft has developed a new way to keep customers informed about security vulnerabilities that affect their Azure resources. When a vulnerability is disclosed that affects their resources, customers will be notified through [Service Health](#) in the Azure Portal. This Service Health message will include information about the vulnerability's common vulnerabilities and exposures number (CVE), severity, and steps customers can take to safeguard against it. In most cases, it will also include a list of the specific resources in their subscription that customers need to take action on.
- Learn more at
- [Understanding Service Health communications for Azure vulnerabilities](#)
- [Azure Service Health Overview](#)
- [Stay informed about Azure security issues - Azure Service Health](#)

