Microsoft

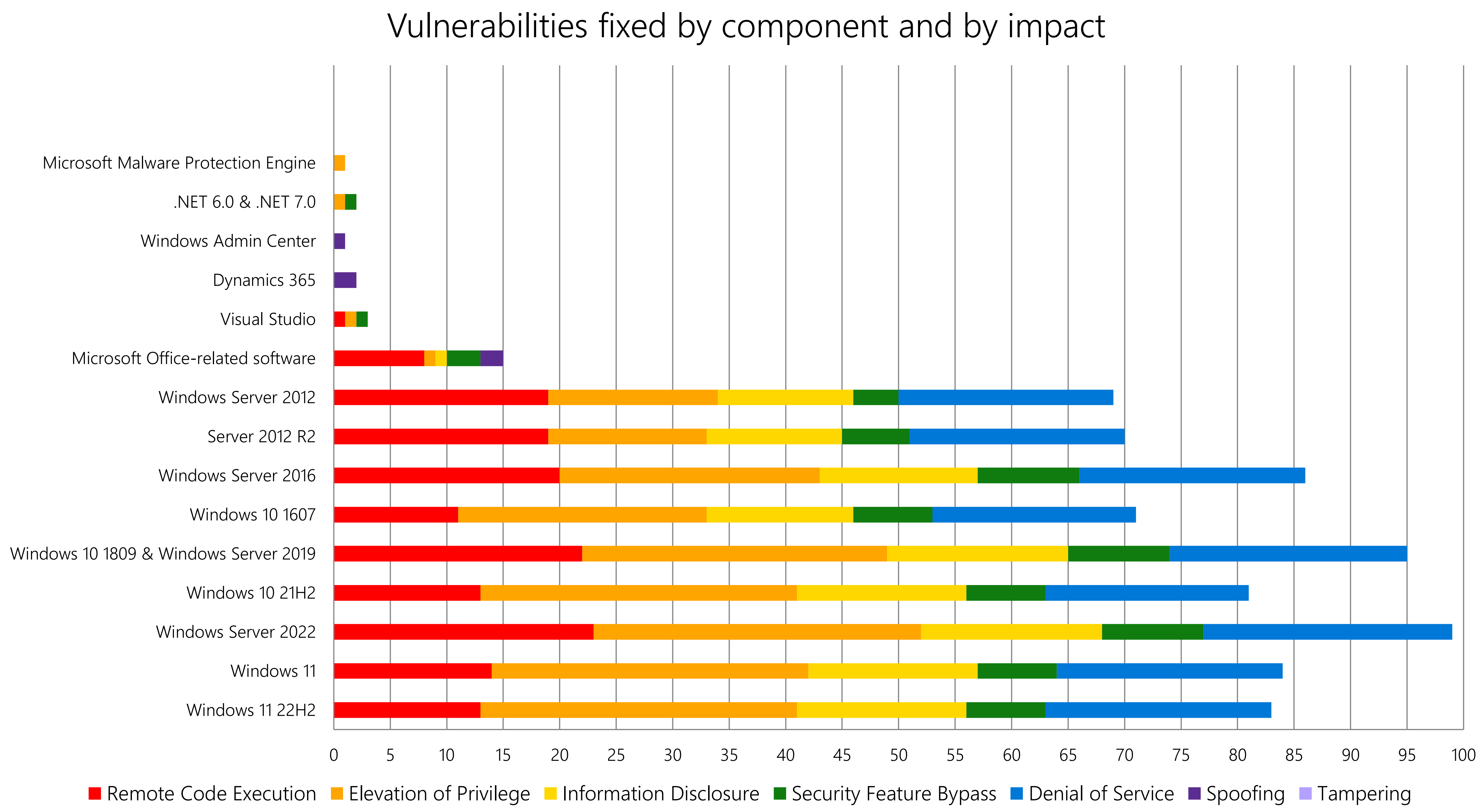
Microsoft Security Release

July 11, 2023

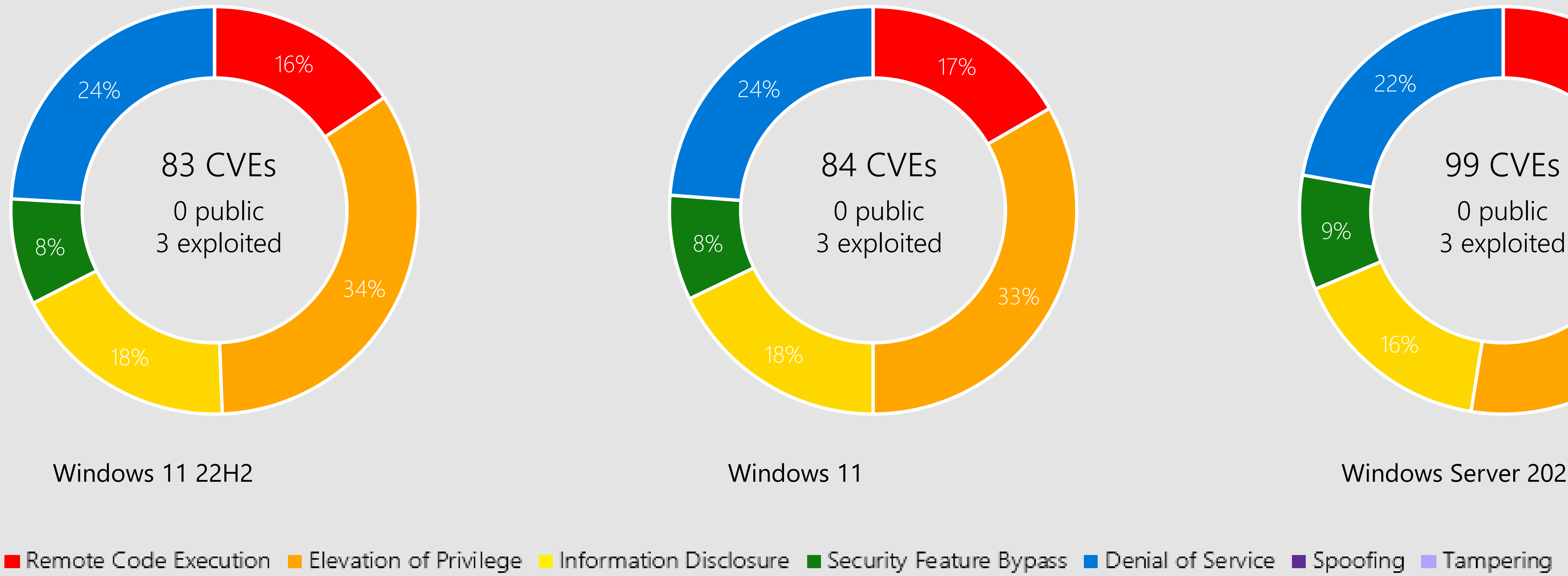
Agenda

- Security Updates
- Security Advisories
- Product Support Lifecycle
- Other resources related to the release

Monthly Security Release Overview - July 2023



Windows 11, Server 2022



Windows 11 22H2

Windows 11

Windows 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-2023-32057 Message Queuing

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

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

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

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-35365 RRAS

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

This vulnerability is only exploitable on Windows Servers that have installed and configured the Routing and Remote Access Service (RRAS) role which is not installed and configured by default.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-32049 SmartScreen

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

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 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016

CVE-2023-32046 MSHTML Platform

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: 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 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-36874 Error Reporting Service

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

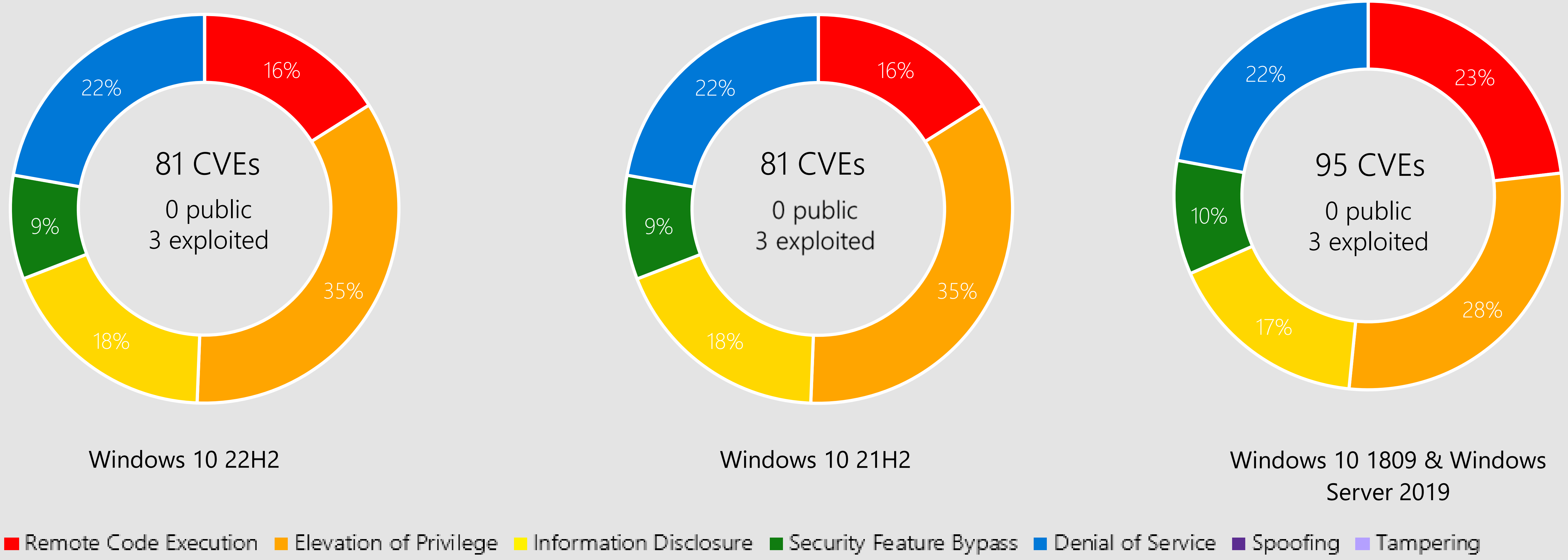
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

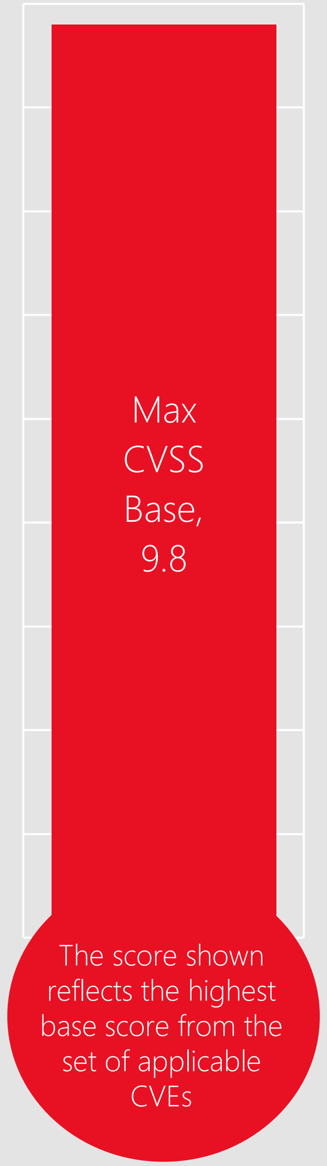
Windows 10



Windows 10 22H2

Windows 10 21H2

Windows 10 1809 & Windows Server 2019



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-2023-35302 Printer Drivers

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

Disable Print Spooler or disable inbound remote printing via GPO. See CVE entry for details.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Windows 10
Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-35303 USB Audio Class System Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: 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 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-35315 Layer-2 Bridge Network Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10

CVE-2023-35364 Kernel

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Windows 10
Server 2022
Server 2019

CVE-2023-35300 Remote Procedure Call Runtime

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

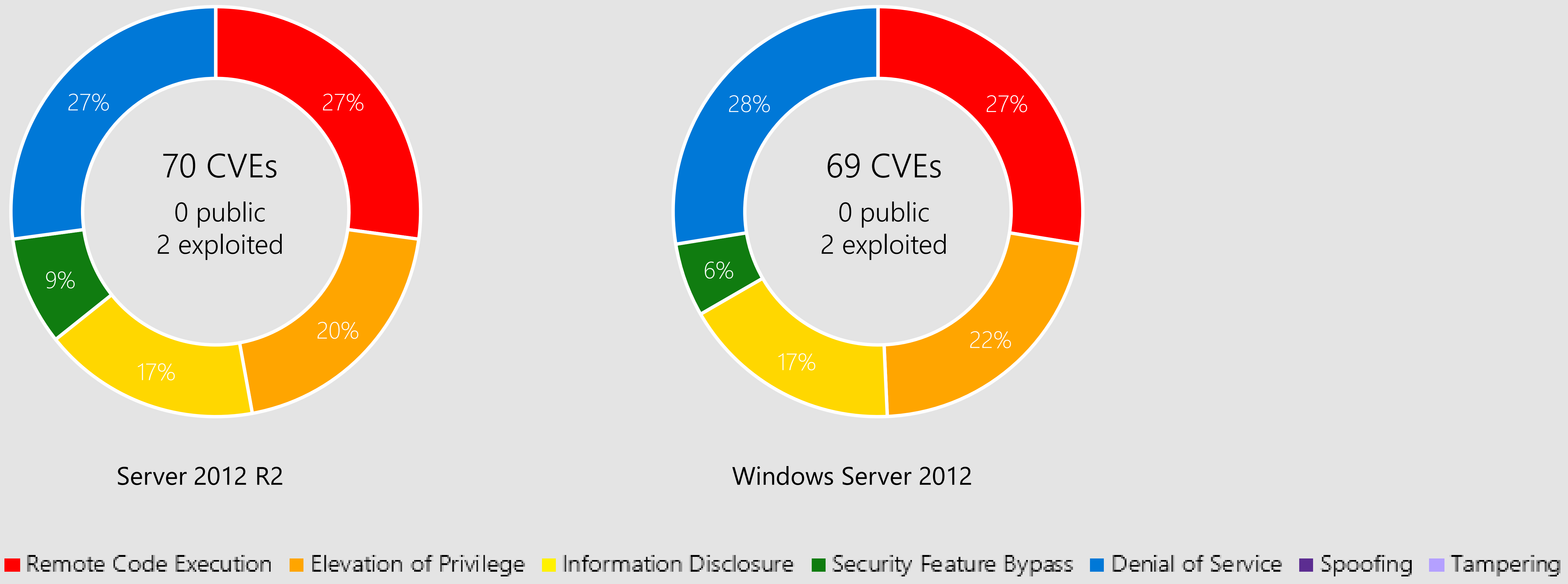
Workarounds

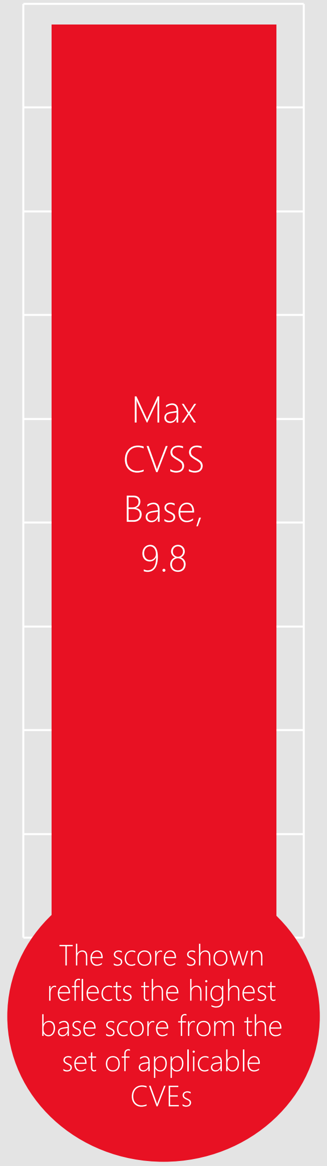
Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

Server 2012 R2, and Server 2012





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

Affected Components:

See Appendix for details

CVE-2023-35322 Deployment Services

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: 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
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-32038 ODBC Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Exploitation of this vulnerability requires an attacker to trick or convince the victim into connecting to their malicious server. If your environment only connects to known, trusted servers and there is no ability to reconfigure existing connections to point to another location (e.g., you use TLS encryption with certificate validation), the vulnerability cannot be exploited.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-35352 Remote Desktop

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.5 | 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 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-29347 Admin Center

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.7 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

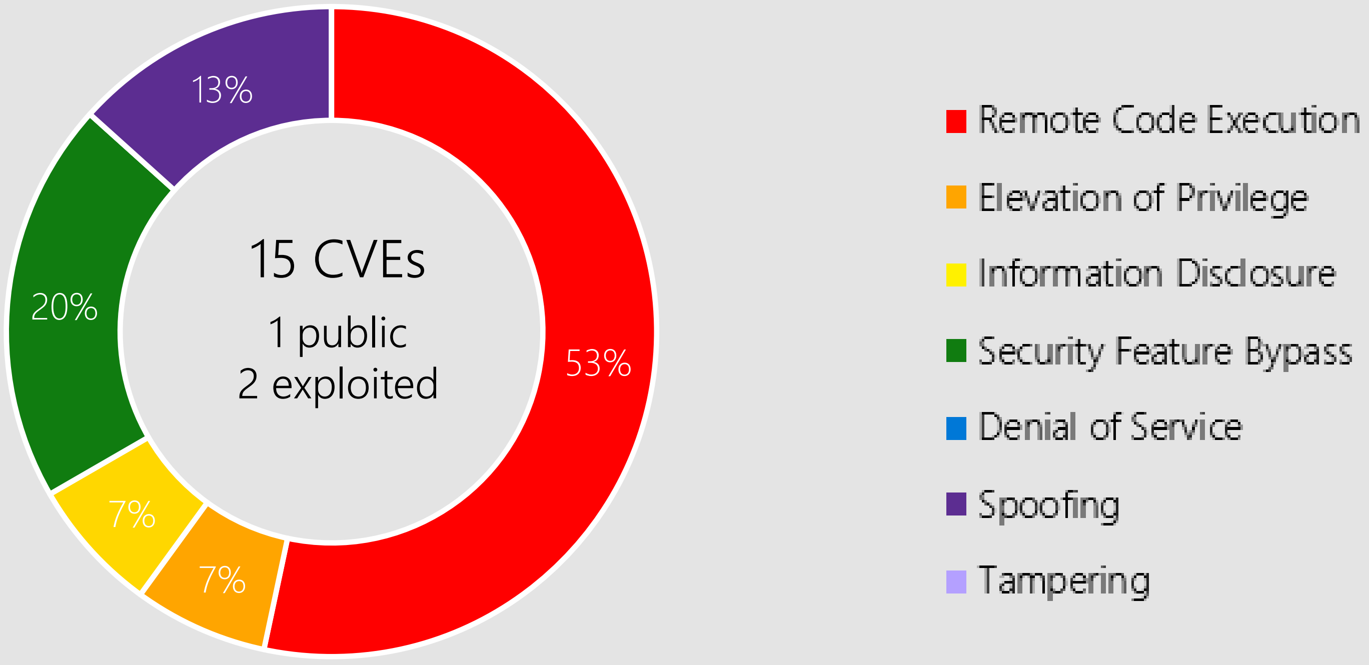
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows Admin Center

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2013 Click-to-Run (C2R)/2016/2019
Word 2013/2016
Outlook 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office Universal
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
SharePoint Server Subscription Edition

CVE-2023-36884 Office

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 8.3 | Attack Vector: Network | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Set FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION registry key. See CVE entry for details.

More Information

This CVE will be updated with new information and links to security updates when they become available.
Microsoft Threat Intelligence Blog *Storm-0978 attacks reveal financial and espionage activities*

Affected Software

Word 2016
Word 2013
Office LTSC 2021
Office 2019
Windows 11
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-33150 Office

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.6 | 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

Word 2016
Word 2013
Office LTSC 2021
Office 2019
365 Apps Enterprise

CVE-2023-35311 Outlook

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

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

Outlook 2016
Outlook 2013
Office 2019
365 Apps Enterprise
Office LTSC 2021

CVE-2023-33160 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

SharePoint Server Subscription Edition
SharePoint Server 2019
SharePoint Enterprise Server 2016

Other Products

Dynamics 365

CVE-2023-35335 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-33171 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

Other Products

Power Apps

CVE-2023-32052 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Microsoft Power Apps (online)

Other Products

.NET 6.0 and .NET 7.0

CVE-2023-33127 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET 6.0, .NET 7.0 ,Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.0.

CVE-2023-33170 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: .NET 6.0, .NET 7.0 ,Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0.

Other Products

Visual Studio

CVE-2023-33127 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.0, .NET 6.0, .NET 7.0.

CVE-2023-33170 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.6, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0, .NET 6.0, .NET 7.0.

Other Products

Visual Study

CVE-2023-36867 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio Code - GitHub Pull Requests and Issues Extension.

Other Products

Azure Service Fabric for Windows

CVE-2023-36868 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure Service Fabric 9.0 Windows, Azure Service Fabric 9.1 Windows.

Other Products

Microsoft Malware Protection Engine

CVE-2023-33156 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.3
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Malware Protection Engine.

Other Products

Apps and Developer tools

CVE-2023-35333 MediaWiki PandocUpload

CVE-2023-32047/CVE-2023-35374 Paint 3D

CVE-2023-35373 Mono

Guidance on Microsoft Signed Drivers Being Used Maliciously

Summary

Microsoft was recently informed that drivers certified by Microsoft's Windows Hardware Developer Program (MWHDP) were being used maliciously in post-exploitation activity. In these attacks, the attacker gained administrative privileges on compromised systems before using the drivers.

Microsoft has completed its investigation and determined that the activity was limited to the abuse of several developer program accounts and that no Microsoft account compromise has been identified. We've suspended the partners' seller accounts and implemented blocking detections for all the reported malicious drivers to help protect customers from this threat.

Recommended Actions:

Microsoft recommends that all customers install the latest Windows updates and ensure their anti-virus and endpoint detection products are up to date with the latest signatures and are enabled to prevent these attacks.

ADV230001 - Security Update Guide - Microsoft - Guidance on Microsoft Signed Drivers Being Used Maliciously

Microsoft Guidance - Trend Micro EFI Modules

Summary

Trend Micro has released CVE-2023-28005 to address a secure boot bypass. Subsequently Microsoft has released the July Windows security updates to block the vulnerable UEFI modules by using the DBX (UEFI Secure Boot Forbidden Signature Database) disallow list.

To exploit this vulnerability, an attacker would need to have administrative privileges or physical access on a system where Secure Boot is configured to trust the Microsoft Unified Extensible Firmware Interface (UEFI) Certificate Authority (CA).

CVEs released for this issue: CVE-2023-28005 IMPORTANT SECURITY BULLETIN: Secure Boot Bypass Vulnerability in Trend Micro Endpoint Encryption (TMEE) FDE 6.0

Recommended Actions:

Microsoft recommends that all customers install the latest Windows updates

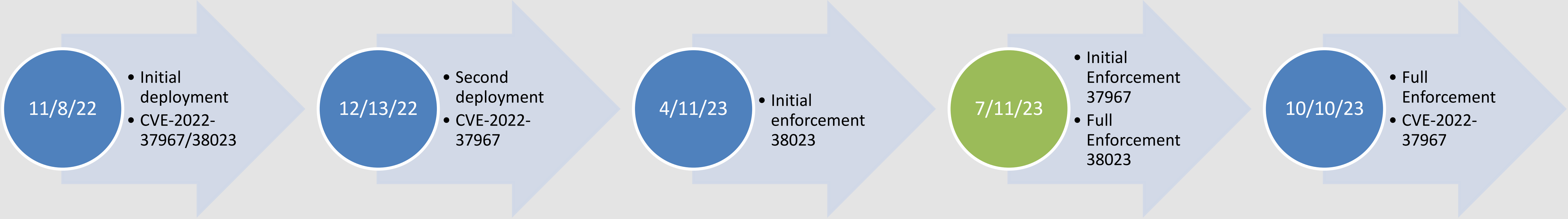
ADV230002 - Security Update Guide - Microsoft - Guidance on Microsoft Signed Drivers Being Used Maliciously

Managing Kerberos and Netlogon Protocol Changes

Summary

Microsoft has published CVE-2022-37966, CVE-2022-38023, and CVE-2022-37967 to address cryptographic protocol vulnerabilities:

- Netlogon, when signing messages using the RC4 cipher.
- Kerberos, when signing messages using the RC4 cipher.
- Kerberos, when using a signature algorithm incorrectly.



11/8/22
- Initial deployment
- CVE-2022-37967/38023

12/13/22
- Second deployment
- CVE-2022-37967

4/11/23
- Initial enforcement 38023

7/11/23
- Initial Enforcement 37967
- Full Enforcement 38023

10/10/23
- Full Enforcement
- CVE-2022-37967

Suggested Actions:

1. Review CVE entries including the FAQ section to understand risks
2. Review the Knowledge Base articles for details on deployment and enforcement of these changes

How to manage Kerberos protocol changes related to CVE-2022-37967 https://support.microsoft.com/help/5020805
How to manage the Kerberos protocol changes related to CVE-2022-37966 https://support.microsoft.com/help/5021131
How to manage Netlogon protocol changes related to CVE-2022-38023 https://support.microsoft.com/help/5021130

Product Lifecycle Update

Products reaching end of support in July

BizTalk Server 2013

BizTalk Server 2013 R2

Visual Studio 2022 , Version 17.0 (LTSC channel)

Dynamics 365 for Customer Engagement Apps, version 9 (on-premises update), Original Release (ver 9.0)

aka.ms/lifecycle

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-21756	No	No	Win32k
CVE-2023-33149	No	No	Office Graphics
CVE-2023-33166	No	No	RPC Runtime
CVE-2023-33167	No	No	RPC Runtime
CVE-2023-33168	No	No	RPC Runtime
CVE-2023-33169	No	No	RPC Runtime
CVE-2023-33172	No	No	RPC Runtime
CVE-2023-33173	No	No	RPC Runtime
CVE-2023-33174	No	No	Cryptographic
CVE-2023-32033	No	No	Failover Cluster
CVE-2023-32034	No	No	RPC Runtime
CVE-2023-32035	No	No	RPC Runtime
CVE-2023-32037	No	No	Layer-2 Bridge Network Driver
CVE-2023-32038	No	No	ODBC Driver

CVE	Public	Exploited	Product
CVE-2023-32041	No	No	Update Orchestrator Service
CVE-2023-32042	No	No	OLE Automation
CVE-2023-32043	No	No	Remote Desktop
CVE-2023-32044	No	No	Message Queuing
CVE-2023-32045	No	No	Message Queuing
CVE-2023-32046	No	Yes	MSHTML Platform
CVE-2023-32049	No	Yes	SmartScreen
CVE-2023-32050	No	No	Installer
CVE-2023-32051	No	No	Raw Image Extension
CVE-2023-35313	No	No	Online Certificate Status Protocol (OCSP) SnapIn
CVE-2023-35314	No	No	RPC Runtime
CVE-2023-35315	No	No	Layer-2 Bridge Network Driver
CVE-2023-35316	No	No	RPC Runtime

CVE	Public	Exploited	Product
CVE-2023-35317	No	No	Server Update Service (WSUS)
CVE-2023-35318	No	No	RPC Runtime
CVE-2023-35319	No	No	RPC Runtime
CVE-2023-35320	No	No	Connected User Experiences and Telemetry
CVE-2023-35321	No	No	Deployment Services
CVE-2023-35322	No	No	Deployment Services
CVE-2023-35323	No	No	OLE
CVE-2023-35325	No	No	Print Spooler
CVE-2023-35326	No	No	CDP User Components
CVE-2023-35328	No	No	Transaction Manager
CVE-2023-35329	No	No	Authentication
CVE-2023-35330	No	No	Extended Negotiation
CVE-2023-35331	No	No	Local Security Authority (LSA)
CVE-2023-35332	No	No	Remote Desktop Protocol

CVE	Public	Exploited	Product
CVE-2023-35336	No	No	MSHTML Platform
CVE-2023-35337	No	No	Win32k
CVE-2023-35338	No	No	Peer Name Resolution Protocol
CVE-2023-35339	No	No	CryptoAPI
CVE-2023-35340	No	No	CNG Key Isolation Service
CVE-2023-35341	No	No	DirectMusic
CVE-2023-35342	No	No	Image Acquisition
CVE-2023-35343	No	No	Geolocation Service
CVE-2023-35344	No	No	DNS Server
CVE-2023-35345	No	No	DNS Server
CVE-2023-35346	No	No	DNS Server
CVE-2023-35347	No	No	Store Install Service
CVE-2023-35350	No	No	Active Directory Certificate Services (AD CS)
CVE-2023-35351	No	No	Active Directory Certificate Services (AD CS)

CVE	Public	Exploited	Product
CVE-2023-35352	No	No	Remote Desktop
CVE-2023-35353	No	No	Connected User Experiences and Telemetry
CVE-2023-35356	No	No	Kernel
CVE-2023-35357	No	No	Kernel
CVE-2023-35358	No	No	Kernel
CVE-2023-35360	No	No	Kernel
CVE-2023-35361	No	No	Kernel
CVE-2023-35362	No	No	Clip Service
CVE-2023-35363	No	No	Kernel
CVE-2023-35364	No	No	Kernel
CVE-2023-35365	No	No	RRAS
CVE-2023-35366	No	No	RRAS
CVE-2023-35367	No	No	RRAS
CVE-2023-36872	No	No	VP9 Video Extensions

CVE	Public	Exploited	Product
CVE-2023-36874	No	Yes	Error Reporting Service
CVE-2023-21526	No	No	Netlogon
CVE-2023-29347	No	No	Admin Center
CVE-2023-33154	No	No	Partition Management Driver
CVE-2023-33155	No	No	Cloud Files Mini Filter Driver
CVE-2023-33156	No	No	Defender
CVE-2023-33163	No	No	Network Load Balancing
CVE-2023-33164	No	No	RPC Runtime
CVE-2023-32053	No	No	Installer
CVE-2023-32054	No	No	Volume Shadow Copy
CVE-2023-32055	No	No	Active Template Library
CVE-2023-32056	No	No	Server Update Service (WSUS)
CVE-2023-32057	No	No	Message Queuing

CVE	Public	Exploited	Product
CVE-2023-32083	No	No	Failover Cluster
CVE-2023-32084	No	No	HTTP.sys
CVE-2023-35297	No	No	PGM
CVE-2023-35298	No	No	HTTP.sys
CVE-2023-35299	No	No	CLFS Driver
CVE-2023-35300	No	No	RPC Runtime
CVE-2023-35303	No	No	USB Audio Class System Driver
CVE-2023-35304	No	No	Kernel
CVE-2023-35305	No	No	Kernel
CVE-2023-35308	No	No	MSHTML Platform
CVE-2023-35309	No	No	Message Queuing
CVE-2023-35310	No	No	DNS Server
CVE-2023-35312	No	No	VOLSNAP.SYS
CVE-2023-36868	No	No	Azure Service Fabric on

CVE	Public	Exploited	Product
CVE-2023-33148	No	No	Office
CVE-2023-33150	No	No	Office
CVE-2023-33151	No	No	Outlook
CVE-2023-33152	No	No	ActiveX
CVE-2023-33153	No	No	Outlook
CVE-2023-33165	No	No	SharePoint Server
CVE-2023-33134	No	No	SharePoint Server
CVE-2023-33157	No	No	SharePoint
CVE-2023-33158	No	No	Excel
CVE-2023-33159	No	No	SharePoint Server
CVE-2023-33160	No	No	SharePoint Server
CVE-2023-33161	No	No	Excel
CVE-2023-33162	No	No	Excel
CVE-2023-35311	No	Yes	Outlook

CVE	Public	Exploited	Product
CVE-2023-32039	No	No	PS and PCL6 Printer Driver
CVE-2023-32040	No	No	PS and PCL6 Printer Driver
CVE-2023-32047	No	No	Paint 3D
CVE-2023-35324	No	No	PS and PCL6 Printer Driver
CVE-2023-35333	No	No	MediaWiki PandocUpload Extension
CVE-2023-35348	No	No	ADFS
CVE-2023-33127	No	No	.NET and Visual Studio
CVE-2023-33170	No	No	ASP.NET and Visual Studio
CVE-2023-33171	No	No	Dynamics 365 (on-premises)
CVE-2023-32052	No	No	Power Apps
CVE-2023-32085	No	No	PS and PCL6 Printer Driver
CVE-2023-35296	No	No	PS and PCL6 Printer Driver
CVE-2023-35302	No	No	PS and PCL6 Printer Driver

CVE	Public	Exploited	Product
CVE-2023-35306	No	No	PS and PCL6 Printer Driver
CVE-2023-35335	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2023-35373	No	No	Mono Authenticode Validation
CVE-2023-35374	No	No	Paint 3D
CVE-2023-36867	No	No	Visual Studio Code GitHub Pull Requests and Issues Extension
CVE-2023-36871	No	No	Azure Active Directory