Microsoft

Microsoft Security Release

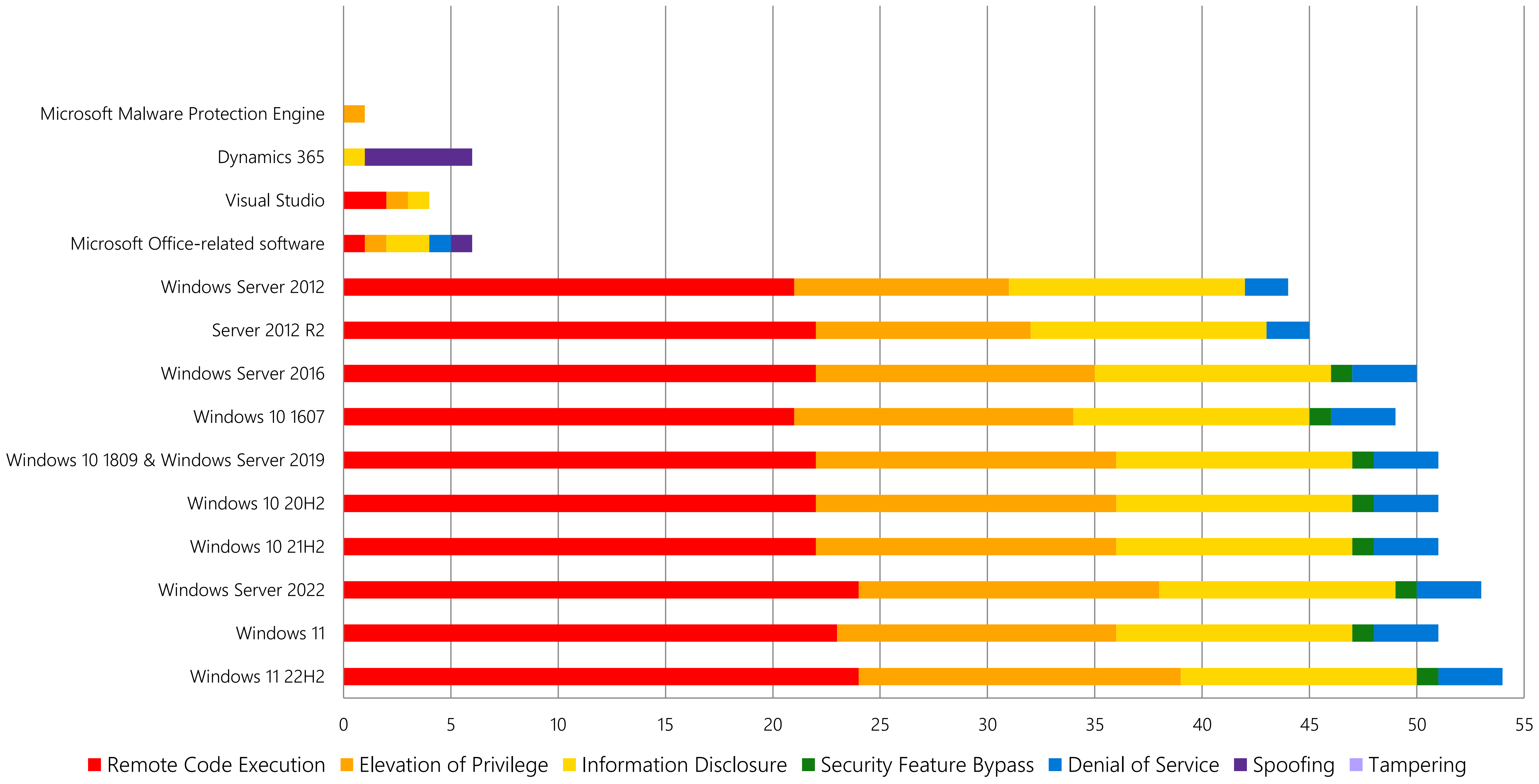
March 14, 2023

Agenda

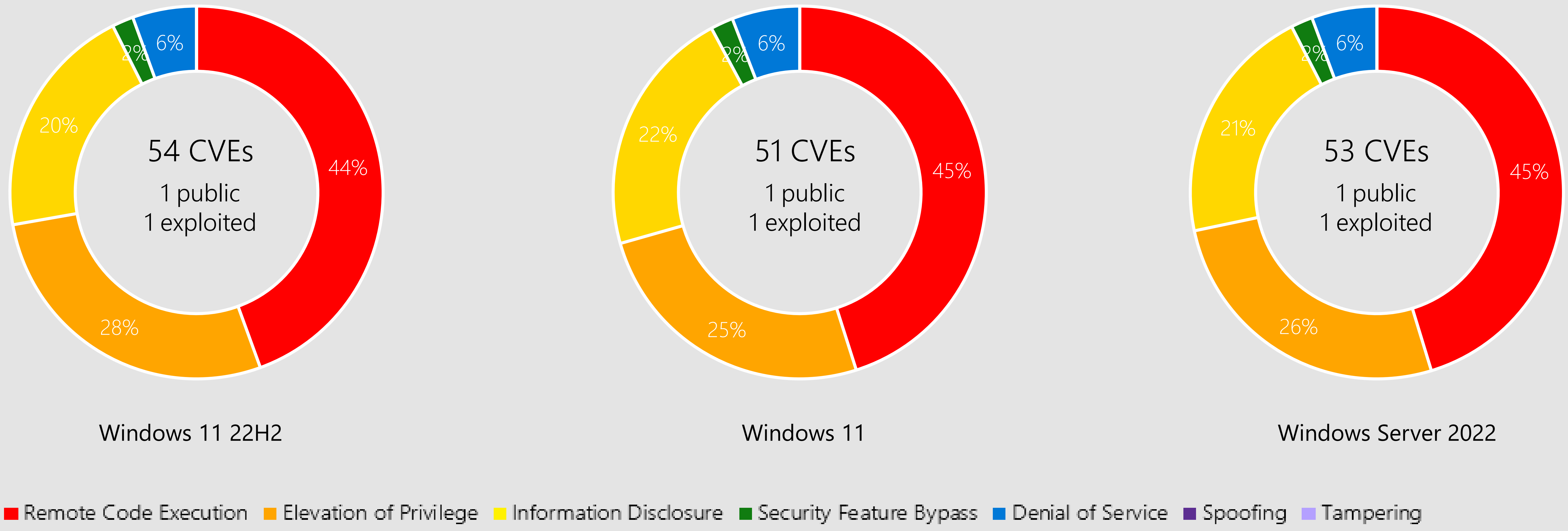
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

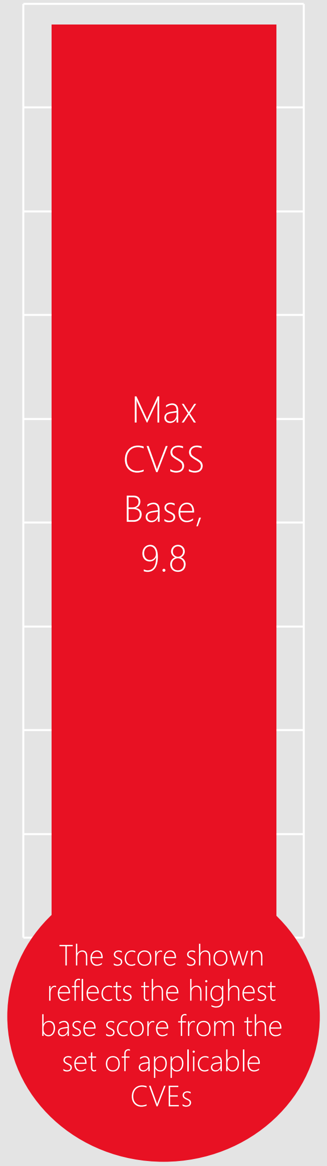
Monthly Security Release Overview - March 2023

Vulnerabilities fixed by component and by impact



Windows 11, Server 2022





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

Affected Components:

Bluetooth Driver
Bluetooth Service
BrokerInfrastructure Service
CSRSS
Cryptographic Services
Graphics Component
Secure Channel
HTTP Protocol Stack
HTTP.sys
Hyper-V
SmartScreen
ICMP
Internet Key Exchange (IKE) Extension
Kernel
Media
Partition Mgmt Driver
PPPoE
Resilient File System (ReFS)
PPTP
PS and PCL6 Class
Printer Driver
RPC Runtime

CVE-2023-21708 RPC Runtime

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-23392 HTTP Protocol Stack

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

A prerequisite for a server to be vulnerable is that the binding has HTTP/3 enabled and the server uses buffered I/O. See CVE entry for details.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11 22H2
Windows 11 version 21H2
Server 2022

CVE-2023-23415 ICMP

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-24864 PS and PCL6 Printer Drivers

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

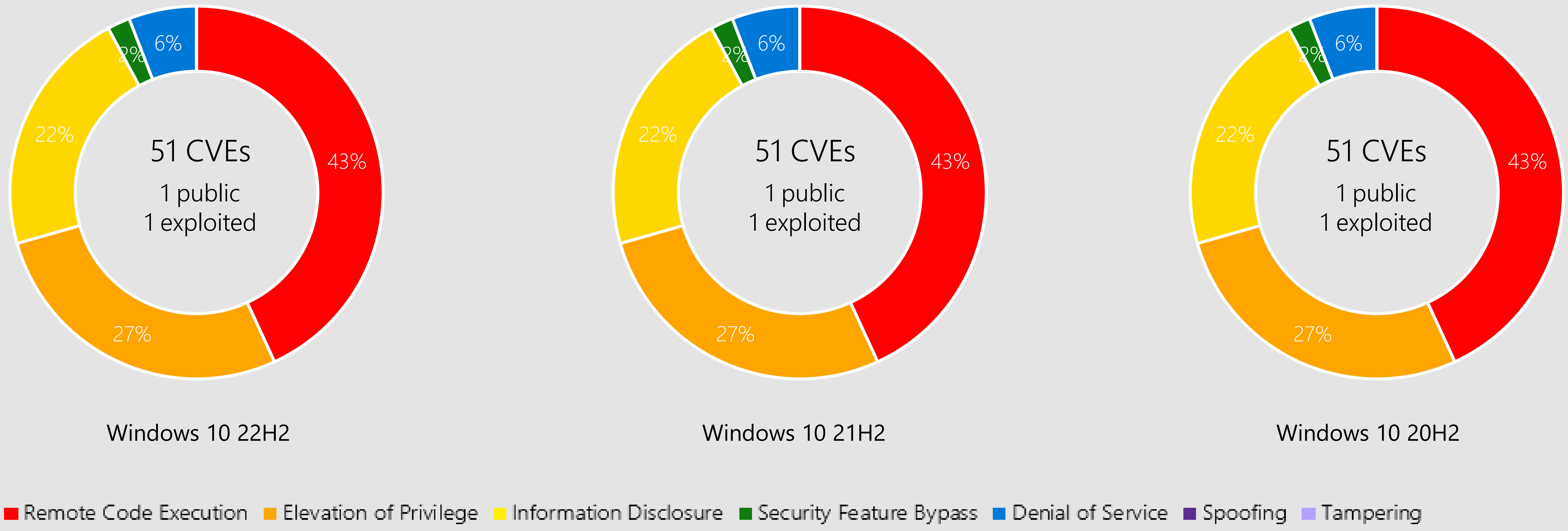
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

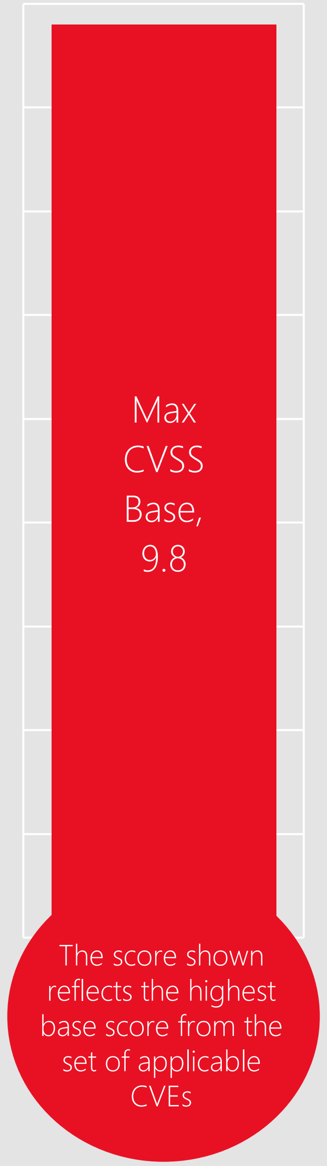
Windows 10



Windows 10 22H2

Windows 10 21H2

Windows 10 20H2



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

Affected Components:

Accounts Picture
Bluetooth Driver
BrokerInfrastructure Service

CSRSS
Cryptographic Services
DNS Server
Secure Channel

Graphics Component
HTTP.sys
Hyper-V
SmartScreen

ICMP
Internet Key Exchange (IKE) Extension
Kernel

Media
Partition Mgmtt Driver
PPPoE
Trusted Platform Module (TPM)

PPTP
PS and PCL6 Class
Printer Driver
RPC Runtime

CVE-2023-24871 Bluetooth Service

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-23388 Bluetooth Driver

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
Server 2022
Windows 10
Server 2016
Server 2019

CVE-2023-1017 TPM 2.0

Impact, Severity, Disclosure

Elevation of Privilege | Critical | 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
Server 2022
Server 2019
Windows 10
Server 2016

CVE-2023-24880 SmartScreen

Impact, Severity, Disclosure

Security Feature Bypass | Moderate | Publicly Disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 5.4 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

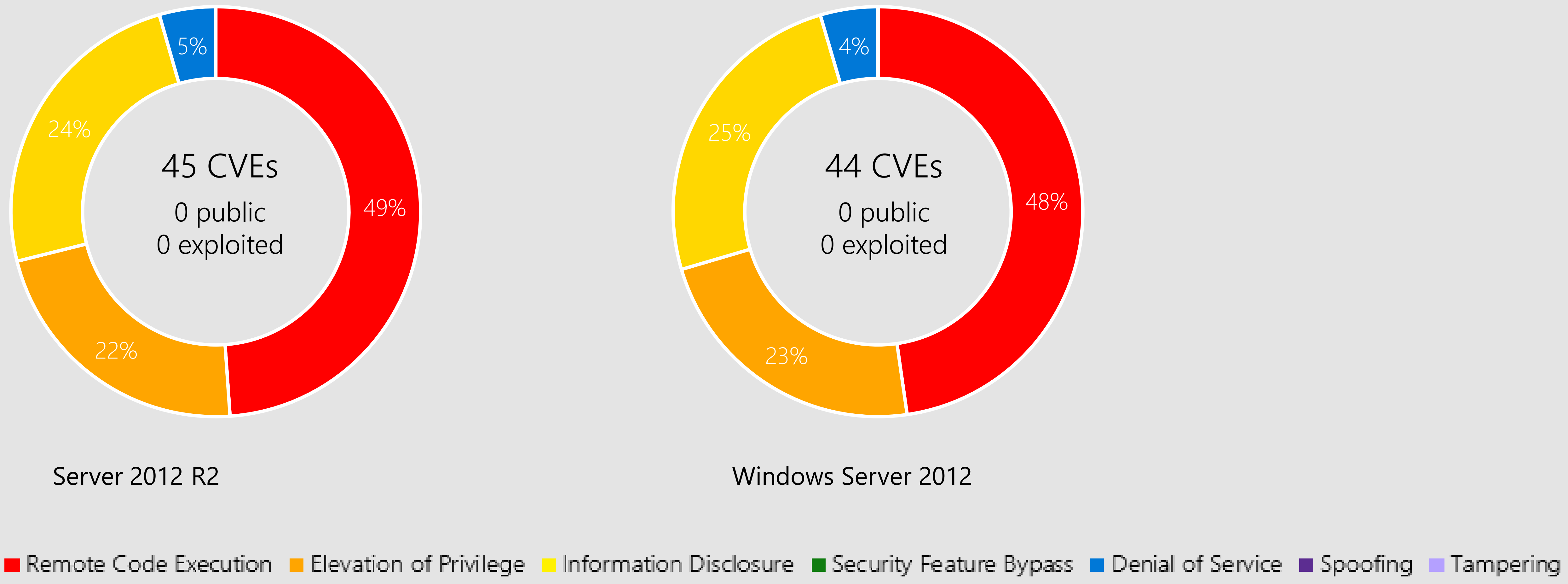
Workarounds

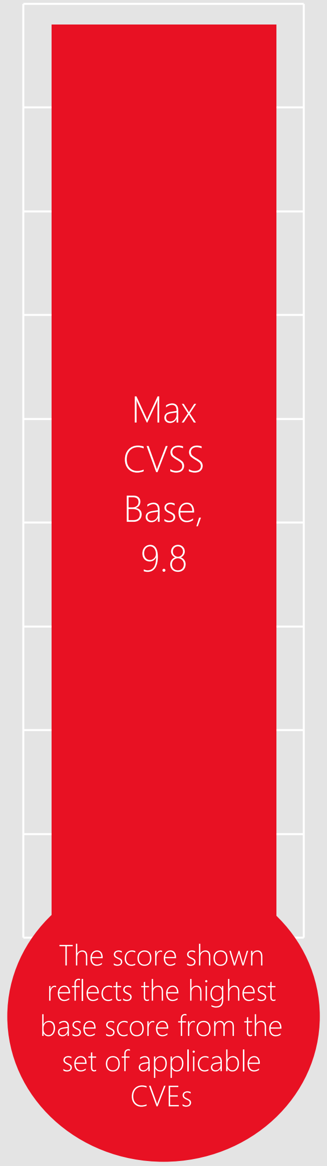
Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

Server 2012 R2 Server 2012





Max CVSS Base, 9.8

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

Affected Components:

- Accounts Picture
- Client Server Run-Time Subsystem (CSRSS)
- Cryptographic Services
- DNS Server
- Graphics Component
- HTTP.sys
- Internet Control Message Protocol (ICMP)
- Internet Key Exchange (IKE) Extension
- Kernel
- Media
- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Tunneling Protocol
- PostScript and PCL6 Class Printer Driver
- Remote Procedure Call Runtime
- Secure Channel

CVE-2023-23416 Cryptographic Services

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.4 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

CVE-2023-23404 Point-to-Point Tunneling Protocol

Impact, Severity, Disclosure

Remote Code Execution | Critical | 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 22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

CVE-2023-23400 DNS Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

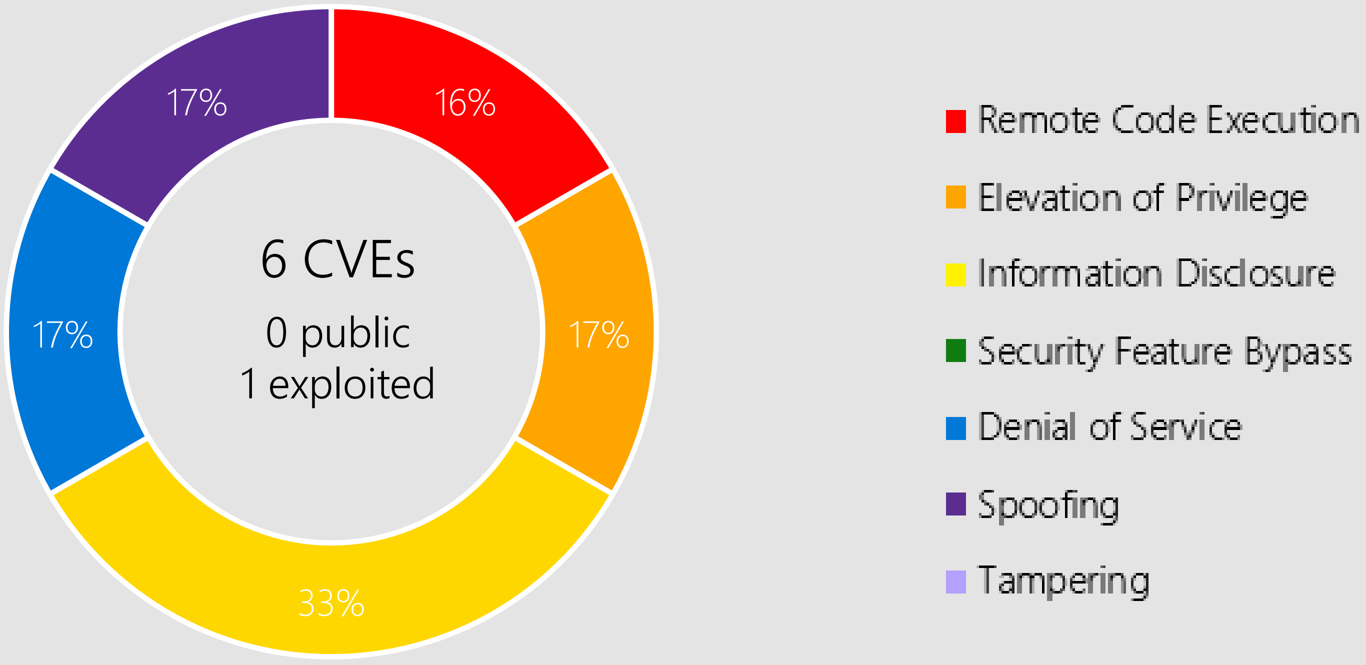
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server 2019
Server 2016
Server 2012 R2

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Outlook 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office Android
Office Universal
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
OneDrive Android
OneDrive for MacOS Installer
SharePoint Foundation 2013
SharePoint Server Subscription Edition

CVE-2023-23397 Outlook

Impact, Severity, Disclosure

Elevation of Privilege | Critical | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

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

Mitigations

Add users to the Protected Users Security Group
Block TCP 445/SMB outbound
See CVE entry for details

Workarounds

MSRC blog Microsoft Mitigates Outlook Elevation of Privilege Vulnerability | MSRC Blog | Microsoft Security Response Center

Affected Software

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

CVE-2023-23399 Excel

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Office 2016
Excel 2016
Excel 2013
Office Web Apps Server 2013
Office 2013
Office LTSC 2021
Office 2019 for Mac
Office 2019
Office Online Server
Office LTSC for Mac 2021
365 Apps Enterprise

Other Products

Dynamics 365

CVE-2023-24879 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-24891 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Dynamics 365

CVE-2023-24919 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-24920 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

Other Products

Dynamics 365

CVE-2023-24921 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 4.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2023-24922 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

Other Products

Microsoft Malware Protection Engine

CVE-2023-23389 | 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

Visual Studio

CVE-2023-22490 | Important | Information Disclosure | Public: No | Exploited: No

CVE details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22490

Products: Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0.

CVE-2023-22743 | Important | Elevation of Privilege | Public: No | Exploited: No

CVE details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22743

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Visual Studio

CVE-2023-23618 | Important | Remote Code Execution | Public: No | Exploited: No

CVE details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23618

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-23946 | Important | Remote Code Execution | Public: No | Exploited: No

CVE details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23946

Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Azure and Store Apps

CVE-2023-23408 Azure HDInsights

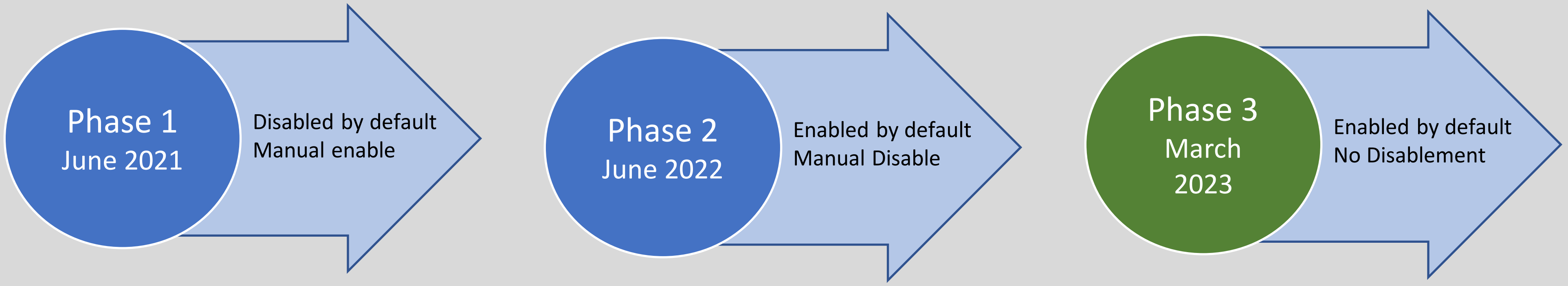
CVE-2023-23383 Azure Service Fabric 9.1 Windows, Azure Service Fabric 9.1 Ubuntu

CVE-2023-24890 OneDrive iOS

Windows DCOM Server Security Hardening

Summary

Microsoft is enforcing Hardening changes in the Distributed Component Object Model (DCOM) for CVE-2021-26414.



- Phase 3 will release in March of 2023 and enables hardening by default but removes the ability to make manual changes.
- This change is permanent, there is no work around or way to bypass/disable these changes.
- Microsoft released a patch which automatically fixes the issue for unhardened Windows based apps in November 2022.

Suggested Actions:

- Fully patch your enterprise up to the March 2023 cumulative security update to ensure your system is secure against this vulnerability.
- Review the Knowledge Base article to understand the implications of these changes ad how to determine if your system is ready. KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass

Product Lifecycle Update

No products retiring in March

Major products retiring April 2023

Exchange 2013
Office 2013

aka.ms/lifecycle

[Latest Servicing Stack Updates]

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-23385	No	No	Point-to-Point Protocol over Ethernet (PPPoE)
CVE-2023-23388	No	No	Bluetooth Driver
CVE-2023-23389	No	No	Defender
CVE-2023-23392	No	No	HTTP Protocol Stack
CVE-2023-23393	No	No	BrokerInfrastructure Service
CVE-2023-21708	No	No	Remote Procedure Call Runtime
CVE-2023-23400	No	No	DNS Server
CVE-2023-23401	No	No	Media
CVE-2023-23402	No	No	Media
CVE-2023-23404	No	No	Point-to-Point Tunneling Protocol
CVE-2023-23405	No	No	Remote Procedure Call Runtime
CVE-2023-23407	No	No	Point-to-Point Protocol over Ethernet (PPPoE)

CVE	Public	Exploited	Product
CVE-2023-23412	No	No	Accounts Picture
CVE-2023-23414	No	No	Point-to-Point Protocol over Ethernet (PPPoE)
CVE-2023-23416	No	No	Cryptographic Services
CVE-2023-23417	No	No	Partition Management Driver
CVE-2023-23418	No	No	Resilient File System (ReFS)
CVE-2023-23419	No	No	Resilient File System (ReFS)
CVE-2023-23420	No	No	Kernel
CVE-2023-23421	No	No	Kernel
CVE-2023-23422	No	No	Kernel
CVE-2023-23423	No	No	Kernel
CVE-2023-24859	No	No	Internet Key Exchange (IKE) Extension
CVE-2023-24861	No	No	Graphics Component
CVE-2023-24862	No	No	Secure Channel
CVE-2023-24908	No	No	Remote Procedure Call Runtime

CVE	Public	Exploited	Product
CVE-2023-24869	No	No	Remote Procedure Call Runtime
CVE-2023-24910	No	No	Graphics Component
CVE-2023-24871	No	No	Bluetooth Service
CVE-2023-24873	No	No	Trusted Platform Module (TPM)
CVE-2023-24880	Yes	Yes	SmartScreen
CVE-2023-22743	No	No	GitHub: CVE-2023-22743 Git for Installer
CVE-2023-23618	No	No	GitHub: CVE-2023-23618 Git for
CVE-2023-23391	No	No	Office for Android
CVE-2023-23395	No	No	SharePoint Server
CVE-2023-23396	No	No	Excel
CVE-2023-23397	No	Yes	Outlook
CVE-2023-23398	No	No	Excel
CVE-2023-23399	No	No	Excel

CVE	Public	Exploited	Product
CVE-2023-23383	No	No	Service Fabric Explorer
CVE-2023-23394	No	No	Client Server Run-Time Subsystem (CSRSS)
CVE-2023-23403	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24856	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24919	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2023-24879	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2023-24920	No	No	Dynamics 365 (on-premises) Cross-site Scripting
CVE-2023-24921	No	No	Dynamics 365 (on-premises) Cross-site Scripting

CVE	Public	Exploited	Product
CVE-2023-23406	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-23408	No	No	Azure Apache Ambari
CVE-2023-23409	No	No	Client Server Run-Time Subsystem (CSRSS)
CVE-2023-23413	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-23415	No	No	Internet Control Message Protocol (ICMP)
CVE-2023-24857	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24858	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24863	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24864	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24865	No	No	PostScript and PCL6 Class Printer Driver

CVE	Public	Exploited	Product
CVE-2023-24868	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24909	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24870	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24911	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24872	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24913	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-24876	No	No	PostScript and PCL6 Class Printer Driver
CVE-2023-23946	No	No	GitHub: CVE-2023-23946 Git path traversal vulnerability
CVE-2023-24890	No	No	OneDrive for iOS