Microsoft

Microsoft Security Release

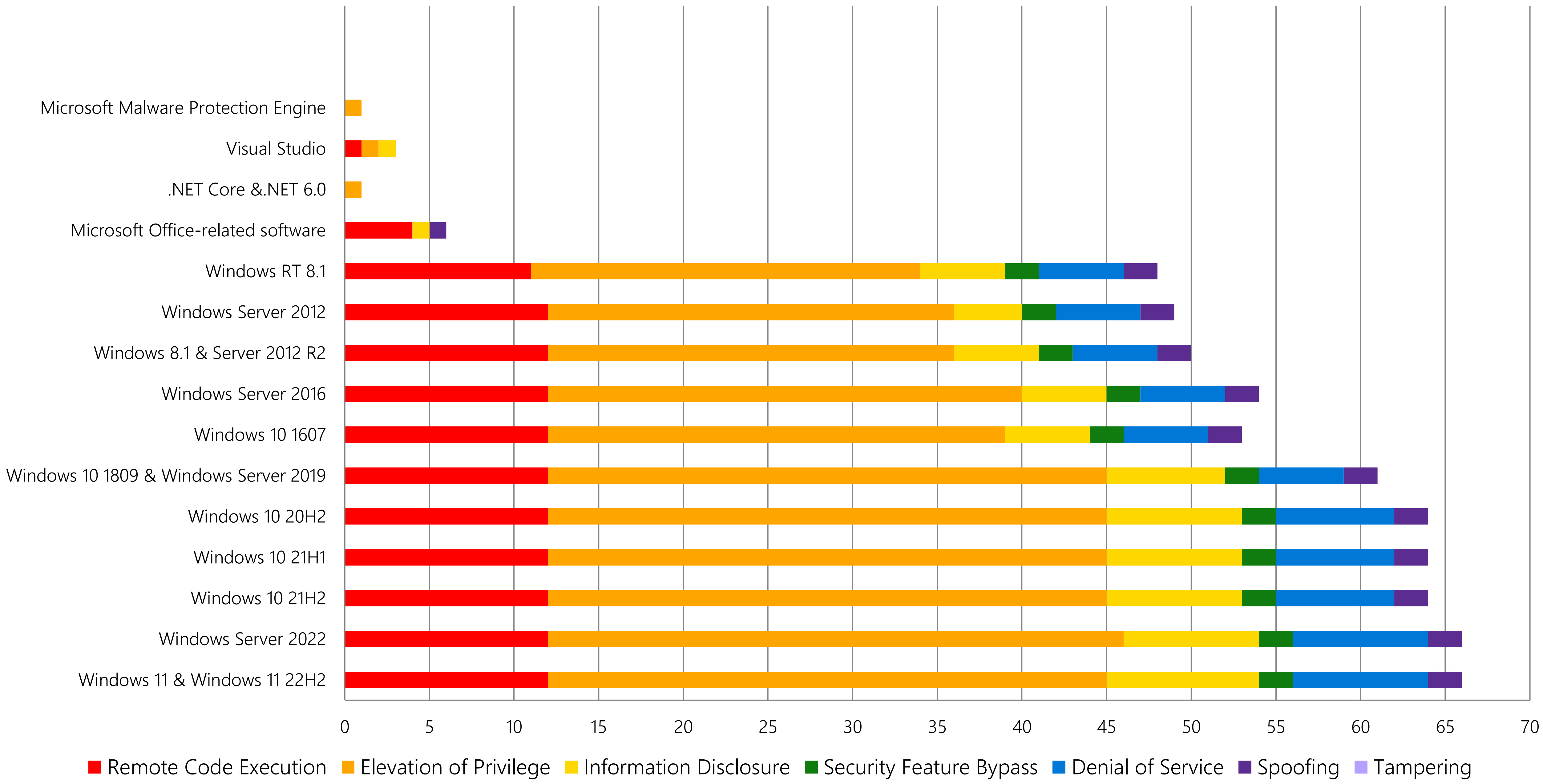
October 11, 2022

Agenda

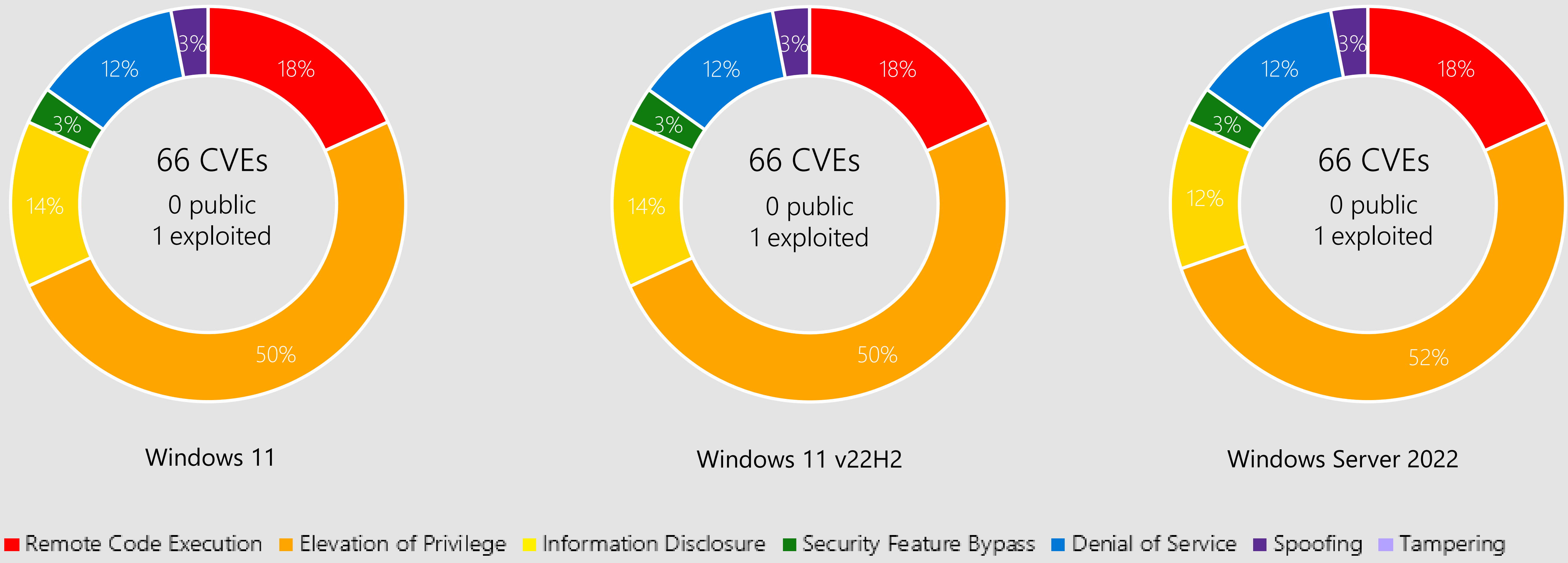
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

Monthly Security Release Overview - October 2022

Vulnerabilities fixed by component and by impact



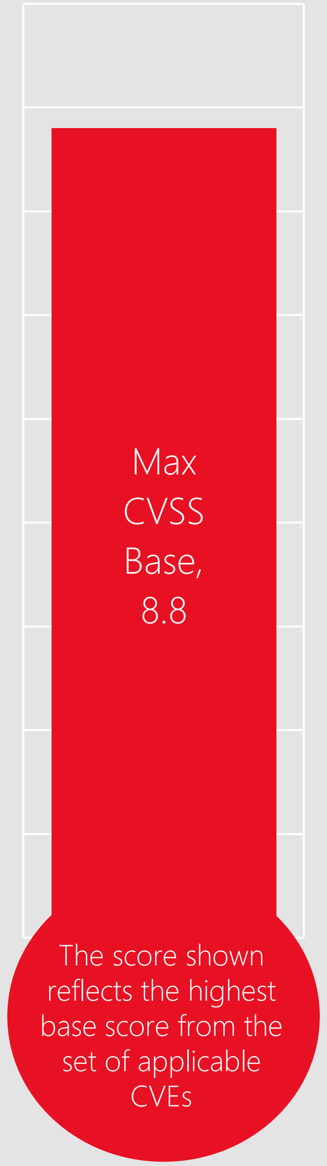
Windows 11, Server 2022



Windows 11

Windows 11 v22H2

Windows Server 2022



Max CVSS Base, 8.8

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

Affected Components:

Please see Appendix for complete list.

CVE-2022-41033 COM+ Event System 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
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-38000 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
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-37982 WDAC OLE DB provider

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.

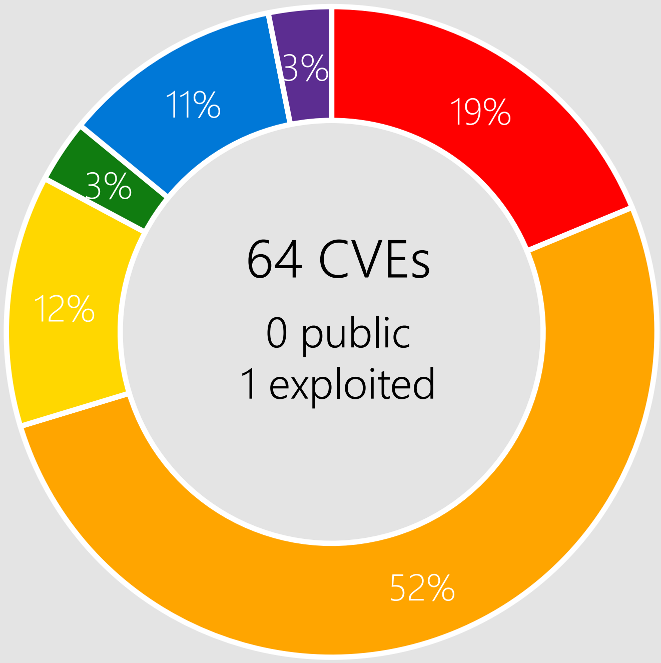
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

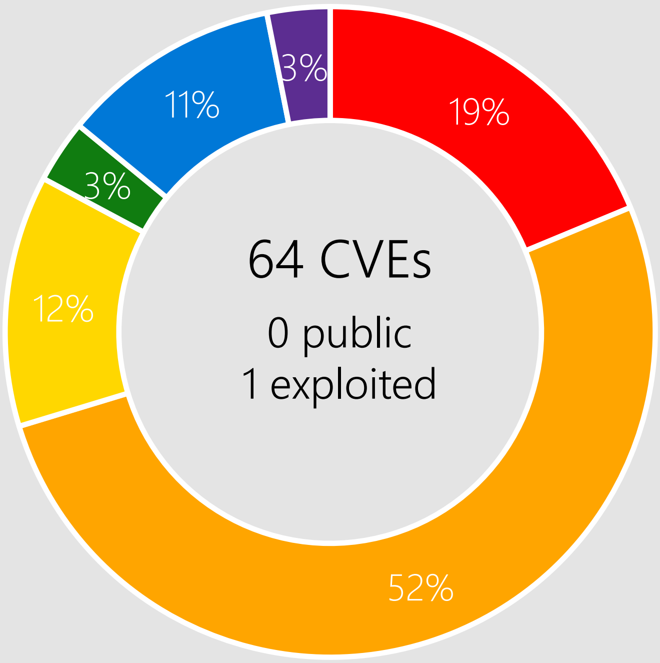
Affected Software

Windows 11
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

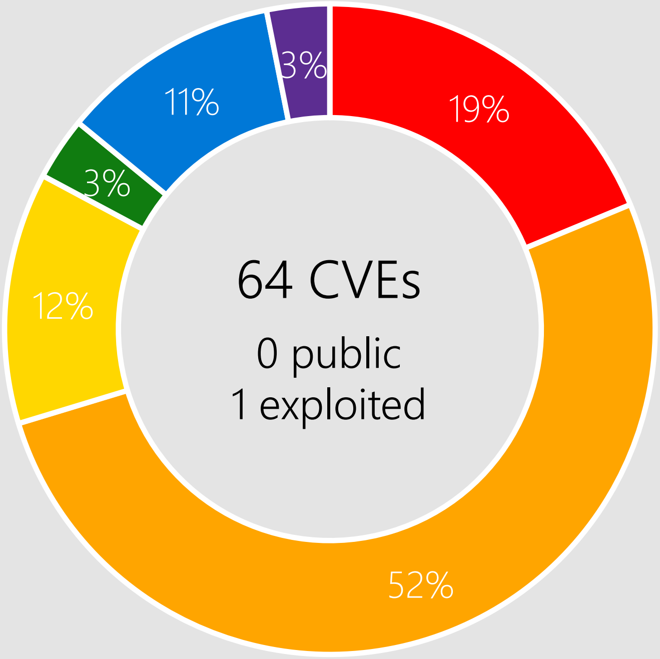
Windows 10



Windows 10 21H2

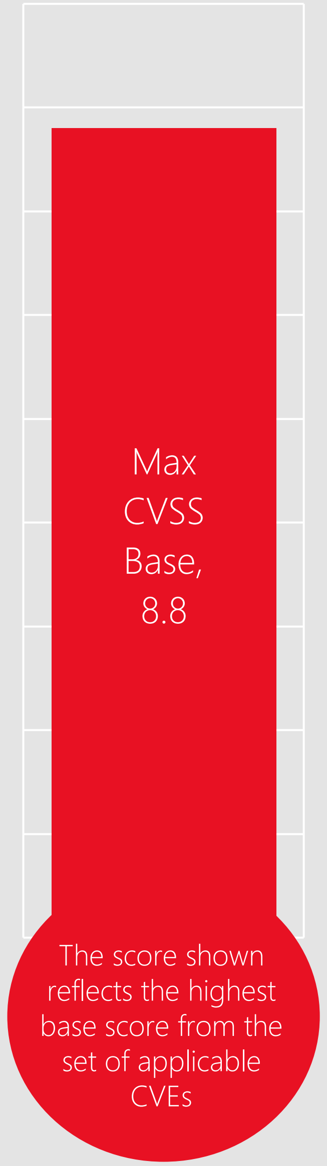


Windows 10 21H1



Windows 10 20H2 & Windows Server v20H2

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



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

Affected Components:

Please see Appendix for complete list.

CVE-2022-37976 Active Directory Certificate Services

Impact, Severity, Disclosure

Elevation of Privilege | 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

A system is vulnerable only if Active Directory Certificate Services is running on the domain.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2022-38016 LSA

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
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-37979 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

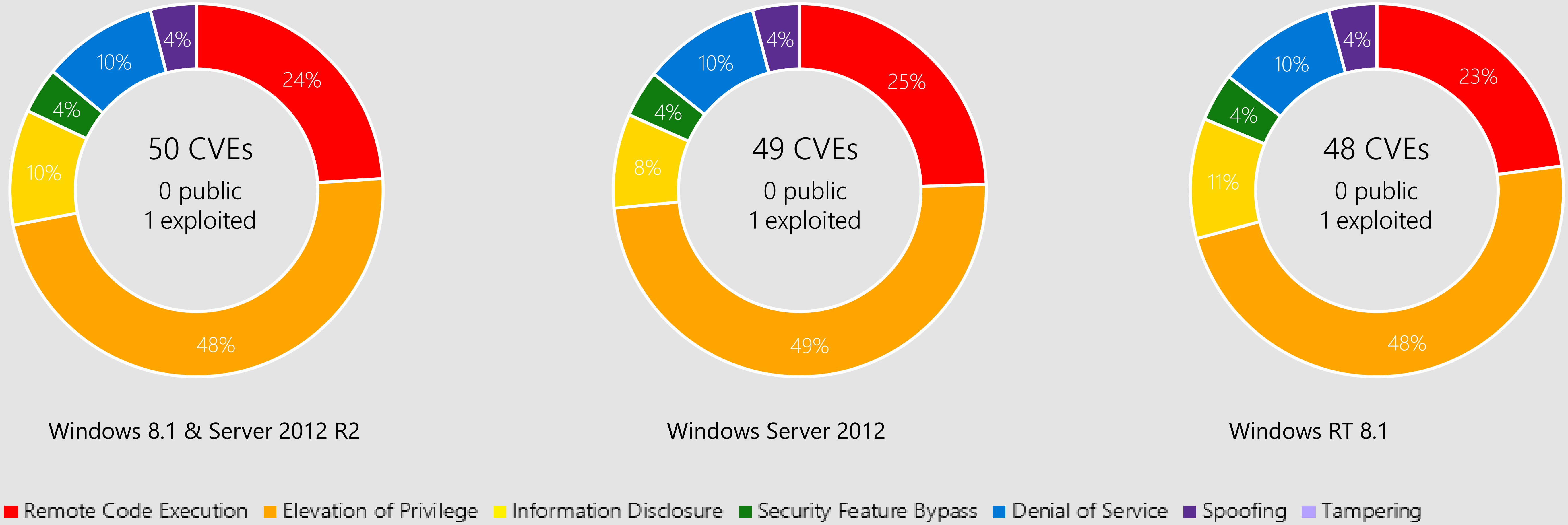
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

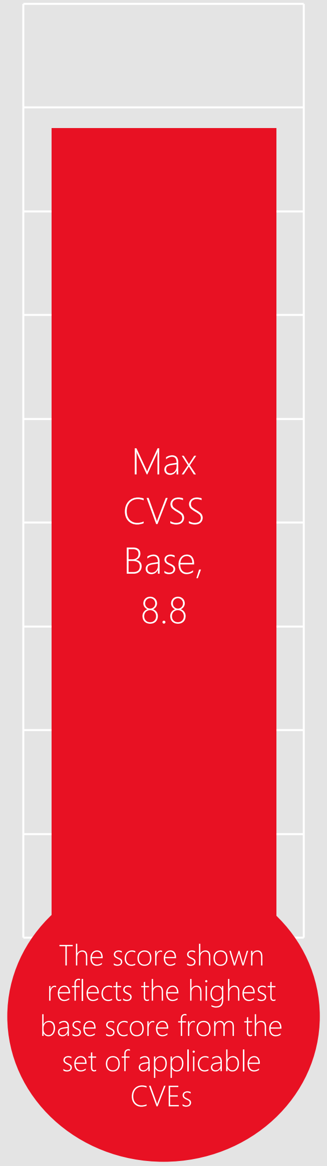
Windows 8.1, Server 2012 R2, and Server 2012



Windows 8.1 & Server 2012 R2

Windows Server 2012

Windows RT 8.1



Max CVSS Base, 8.8

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

Affected Components:

Please see Appendix for complete list.

CVE-2022-38040 ODBC Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-38041 Secure Channel

Impact, Severity, Disclosure

Denial of Service | Important | 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.

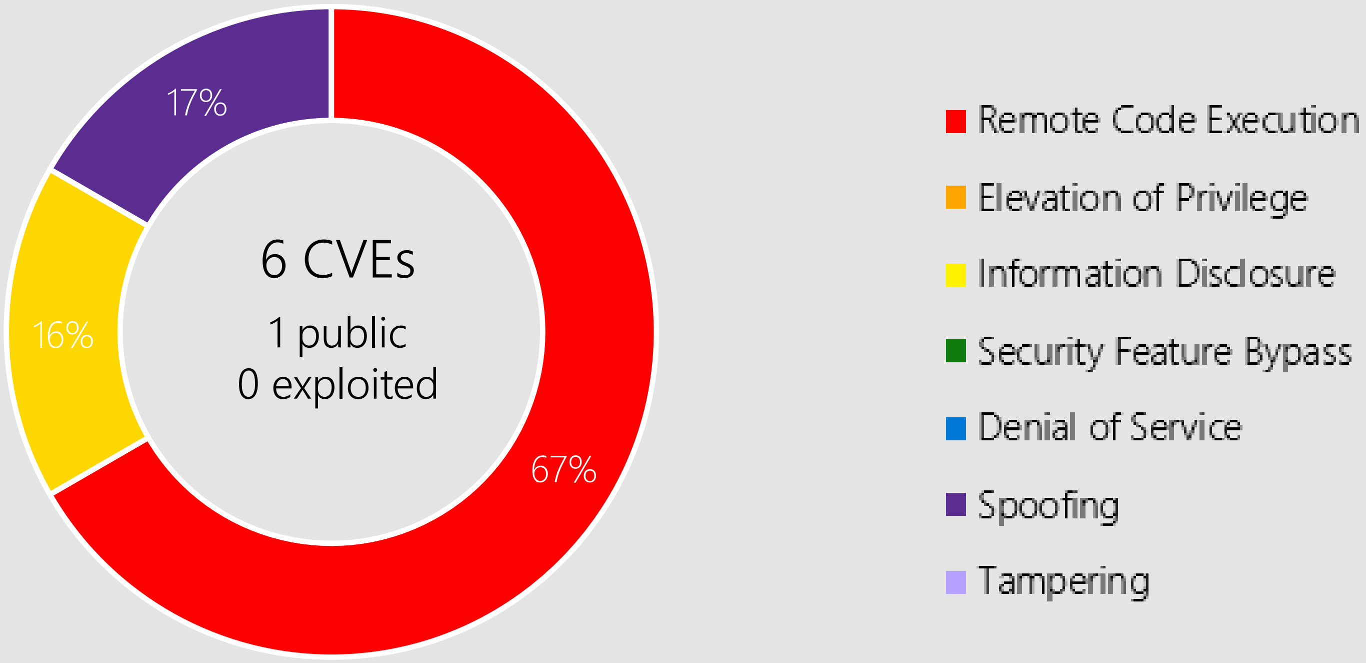
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 11 22H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
SharePoint Foundation 2013
SharePoint Server Subscription Edition

CVE-2022-41038 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 Foundation 2013
SharePoint Server 2019
SharePoint Enterprise Server 2016
SharePoint Enterprise Server 2013

CVE-2022-38049 Office Graphics

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 LTSC 2021
365 Apps Enterprise
Office 2019

Other Products

.NET Core and .NET 6.0

CVE-2022-41032 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: .NET Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.3, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.2, Visual Studio 2022 for Mac version 17.3, .NET 6.0.

Other Products

Visual Studio

CVE-2022-41032 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: .NET Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.3, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.2, Visual Studio 2022 for Mac version 17.3, .NET 6.0.

CVE-2022-41034 | 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.

Other Products

Visual Studio

CVE-2022-41042 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio Code.

CVE-2022-41083 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Jupyter Extension Visual Studio Code.

Other Products

Microsoft Malware Protection Engine

CVE-2022-37971 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Malware Protection Engine.

Other Products

Azure Arc-enabled Kubernetes cluster and Azure Stack Edge

CVE-2022-37968 | Critical | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 10
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Azure Arc-enabled Kubernetes cluster 1.8.11, Azure Arc-enabled Kubernetes cluster 1.7.18, Azure Arc-enabled Kubernetes cluster 1.5.8, Azure Arc-enabled Kubernetes cluster 1.6.19, Azure Stack Edge.

What version of the Azure Arc-enabled Kubernetes cluster addresses this vulnerability?

Version 1.8.14 is safeguarded against this vulnerability. Auto-upgrade is enabled by default for customers using Azure Arc however, if you manually control your updates, action is required to upgrade to the latest version.

How do I check which version of the Azure Arc-enabled Kubernetes cluster I am currently using?

Guidance is available in the Check agent version section of Upgrade Azure Arc-enabled Kubernetes agents.

Other Products

Azure Service Fabric Explorer

CVE-2022-35829 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: Required
Products: Azure Service Fabric Explorer.

How can I ensure I am not on a vulnerable version of Service Fabric Explorer?

A vulnerable version of Service Fabric Explorer (SFXv1) has the URL that ends in "old.html". If you are on an unsupported version of Service Fabric Runtime (8.1.316 and below), you will be vulnerable. Please update to a supported version of Service Fabric Runtime. See Service Fabric supported versions for the list of all supported versions of the runtime. On supported versions of the Service Fabric Runtime, the Service Fabric Explorer version (SFXv2) which is loaded by default is not affected by this vulnerability. On supported SF runtime versions, you can verify you are using SFXv2 by checking that the URL of Service Fabric Explorer ends in "index.html".

Other Products

Azure

CVE-2022-38017 Azure StorSimple 8000 Series

Known Issues

Exchange updates for October

The October 2022 Exchange SUs do not contain fixes for the zero-day vulnerabilities reported publicly on September 29, 2022. We will release updates for CVE-2022-41040 and CVE-2022-41082 vulnerabilities as soon as they are ready.

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-october-2022-exchange-server-security-updates/ba-p/3646263

What is in the October Exchange update(s)?

Addresses known issue of Outlook Probes not functioning properly with extended protection turned on

Product Lifecycle Update

Fixed policy

Forefront Identity Manager 2010

Forefront Identity Manager 2010 R2

SQL Server 2016, Service Pack 2
Visual Studio 2019, Version 16.9

Modern policy

Microsoft Endpoint Configuration Manager, Version 2103

Dynamics 365 Business Central on-premises (Modern Policy), 2021 release wave 1, version 18.x

aka.ms/lifecycle

Windows 8.1 end of support Jan 2023

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-30198	No	No	PPTP
CVE-2022-22035	No	No	PPTP
CVE-2022-24504	No	No	PPTP
CVE-2022-33634	No	No	PPTP
CVE-2022-33635	No	No	GDI+
CVE-2022-33645	No	No	TCP/IP Driver
CVE-2022-34689	No	No	CryptoAPI
CVE-2022-35770	No	No	NTLM
CVE-2022-37965	No	No	PPTP
CVE-2022-37970	No	No	DWM Core Library
CVE-2022-37971	No	No	Defender
CVE-2022-38034	No	No	Workstation Service
CVE-2022-37986	No	No	Win32k
CVE-2022-37987	No	No	CSRSS

CVE	Public	Exploited	Product
CVE-2022-38036	No	No	Internet Key Exchange (IKE) Protocol
CVE-2022-38046	No	No	Web Account Manager
CVE-2022-37998	No	No	Local Session Manager (LSM)
CVE-2022-38047	No	No	PPTP
CVE-2022-37999	No	No	Group Policy Preference Client
CVE-2022-38000	No	No	PPTP
CVE-2022-38049	No	No	Office Graphics
CVE-2022-38050	No	No	Win32k
CVE-2022-38051	No	No	Graphics Component
CVE-2022-38003	No	No	Resilient File System
CVE-2022-41081	No	No	PPTP
CVE-2022-38016	No	No	Local Security Authority (LSA)
CVE-2022-38021	No	No	Connected User Experiences and Telemetry
CVE-2022-37973	No	No	Local Session Manager (LSM)

CVE	Public	Exploited	Product
CVE-2022-38022	No	No	Kernel
CVE-2022-37974	No	No	Mixed Reality Developer Tools
CVE-2022-37975	No	No	Group Policy
CVE-2022-37976	No	No	Active Directory Certificate Services
CVE-2022-38025	No	No	Distributed File System (DFS)
CVE-2022-37977	No	No	Local Security Authority Subsystem Service (LSASS)
CVE-2022-38026	No	No	DHCP Client
CVE-2022-37978	No	No	Active Directory Certificate Services
CVE-2022-38027	No	No	Storage
CVE-2022-37979	No	No	Hyper-V
CVE-2022-38028	No	No	Print Spooler
CVE-2022-37980	No	No	DHCP Client
CVE-2022-38029	No	No	ALPC
CVE-2022-37981	No	No	Event Logging Service

CVE	Public	Exploited	Product
CVE-2022-38030	No	No	USB Serial Driver
CVE-2022-37983	No	No	DWM Core Library
CVE-2022-38032	No	No	Portable Device Enumerator Service
CVE-2022-37984	No	No	WLAN Service
CVE-2022-38033	No	No	Server Remotely Accessible Registry Keys
CVE-2022-37985	No	No	Graphics Component
CVE-2022-37988	No	No	Kernel
CVE-2022-38037	No	No	Kernel
CVE-2022-37989	No	No	Client Server Run-time Subsystem (CSRSS)
CVE-2022-38038	No	No	Kernel
CVE-2022-37990	No	No	Kernel
CVE-2022-38039	No	No	Kernel
CVE-2022-37991	No	No	Kernel
CVE-2022-38040	No	No	ODBC Driver

CVE	Public	Exploited	Product
CVE-2022-38041	No	No	Secure Channel
CVE-2022-37993	No	No	Group Policy Preference Client
CVE-2022-37994	No	No	Group Policy Preference Client
CVE-2022-38043	No	No	Security Support Provider Interface
CVE-2022-37995	No	No	Kernel
CVE-2022-38044	No	No	CD-ROM File System Driver
CVE-2022-37996	No	No	Kernel Memory
CVE-2022-38045	No	No	Server Service Remote Protocol
CVE-2022-37997	No	No	Graphics Component
CVE-2022-41033	No	Yes	COM+ Event System Service

CVE	Public	Exploited	Product
CVE-2022-38048	No	No	Office
CVE-2022-38001	No	No	Office
CVE-2022-41036	No	No	SharePoint Server
CVE-2022-41037	No	No	SharePoint Server
CVE-2022-38053	No	No	SharePoint Server
CVE-2022-41031	No	No	Word

CVE	Public	Exploited	Product
CVE-2022-41038	No	No	SharePoint Server
CVE-2022-41043	Yes	No	Office
CVE-2022-35829	No	No	Service Fabric Explorer
CVE-2022-37968	No	No	Azure Arc-enabled Kubernetes cluster Connect
CVE-2022-38017	No	No	StorSimple 8000 Series
CVE-2022-41032	No	No	NuGet Client
CVE-2022-41034	No	No	Visual Studio Code
CVE-2022-37982	No	No	WDAC OLE DB provider for SQL Server
CVE-2022-38031	No	No	WDAC OLE DB provider for SQL Server
CVE-2022-38042	No	No	Active Directory Domain Services
CVE-2022-41083	No	No	Visual Studio Code
CVE-2022-41042	No	No	Visual Studio Code