Microsoft

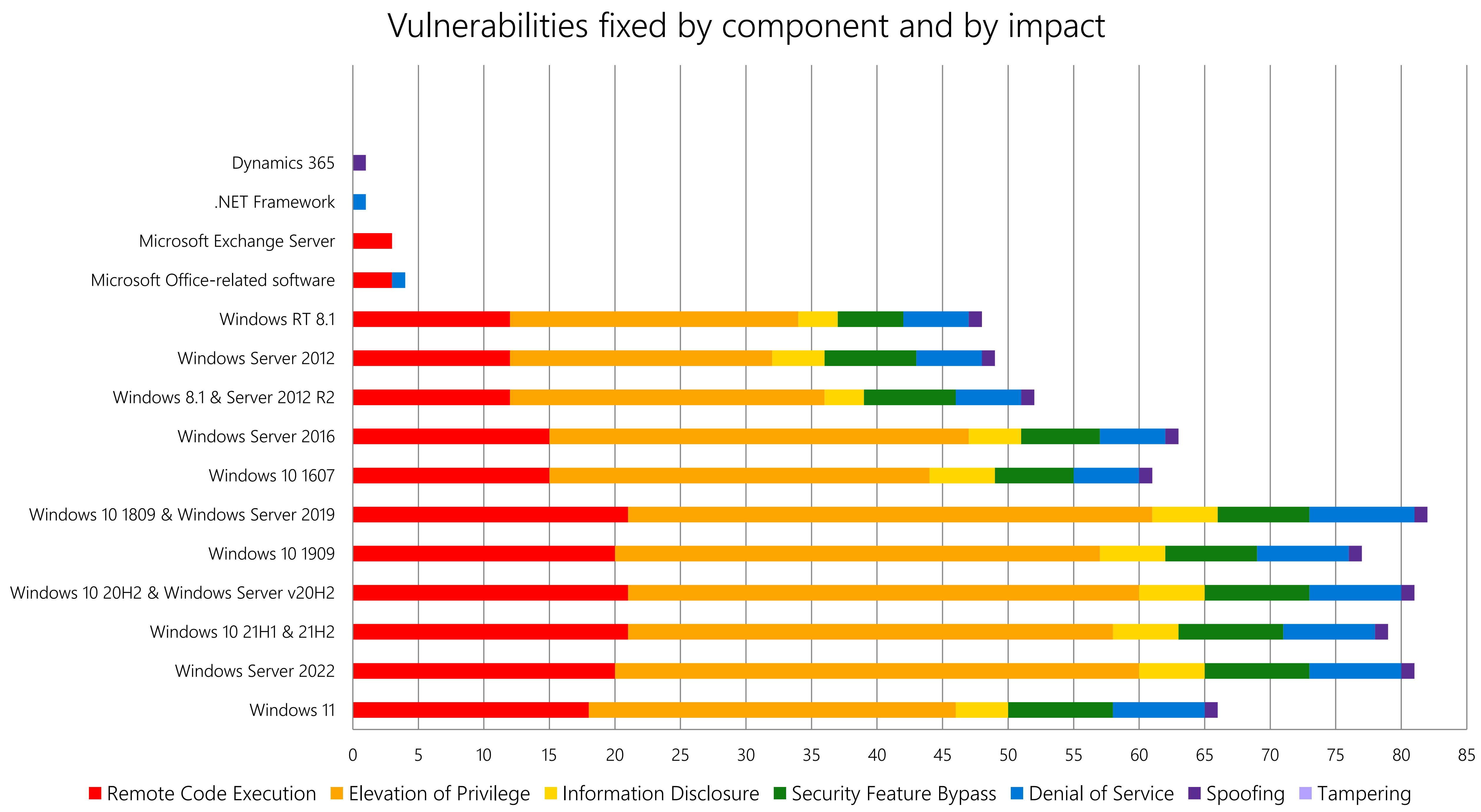
Microsoft Security Release

January 11, 2022

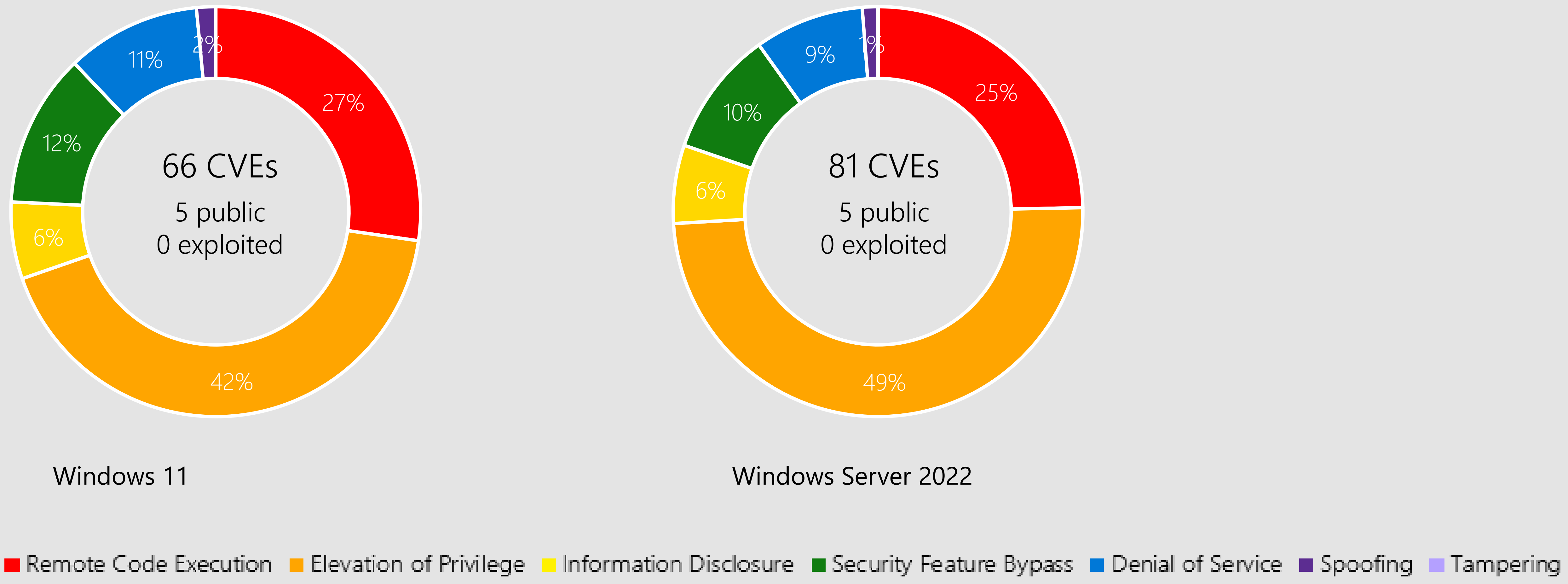
Agenda

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

Monthly Security Release Overview - January 2022

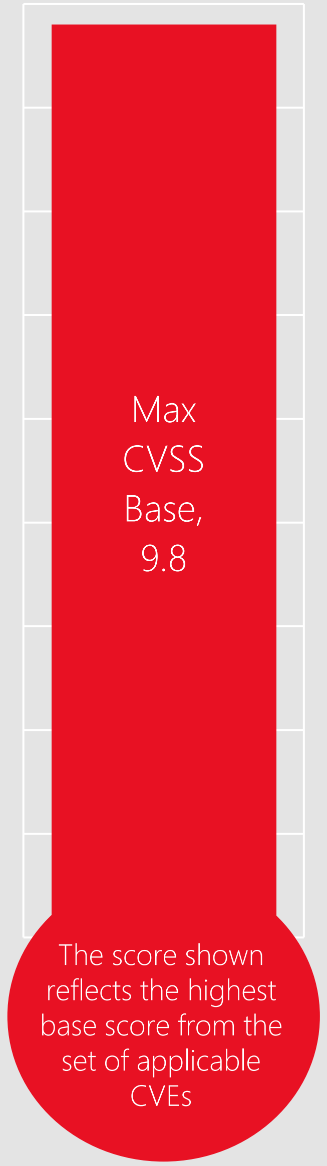


Windows 11, Server 2022



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:

Too many to list. Please see appendix for details.

CVE-2022-21907 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

Windows Server 2019 is not vulnerable in the default configuration. `EnableTrailerSupport` needs to be 'on'. See CVE entry for details.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10

CVE-2022-21893 Remote Desktop Protocol

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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-21849 IKE Extension

Impact, Severity, Disclosure

Remote Code Execution | Important | 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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016

CVE-2022-21922 RPC 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.

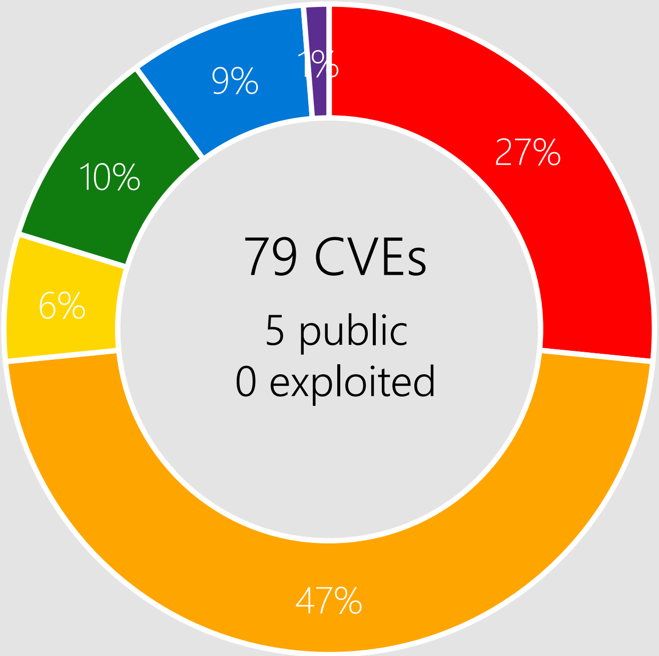
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

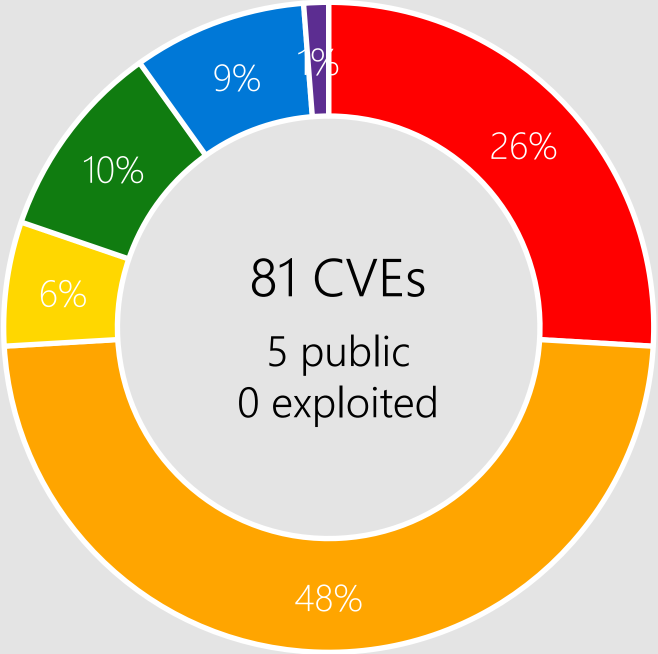
Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

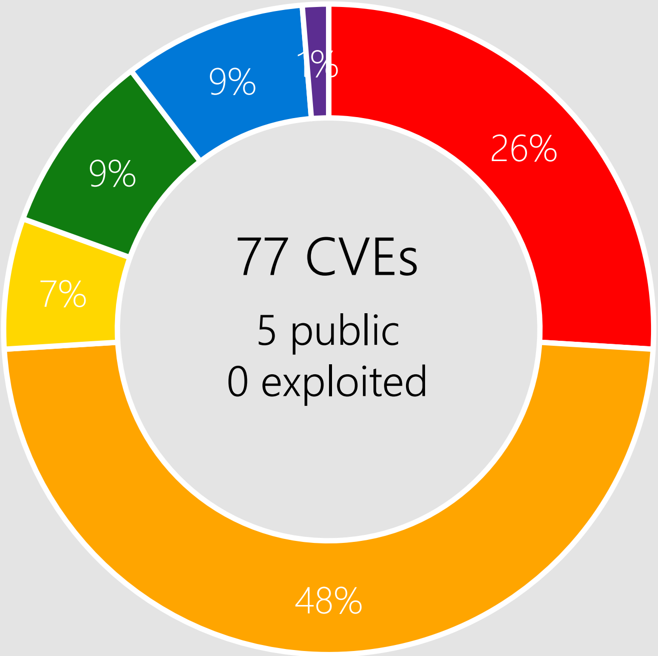
Windows 10



Windows 10 21H1 & 21H2

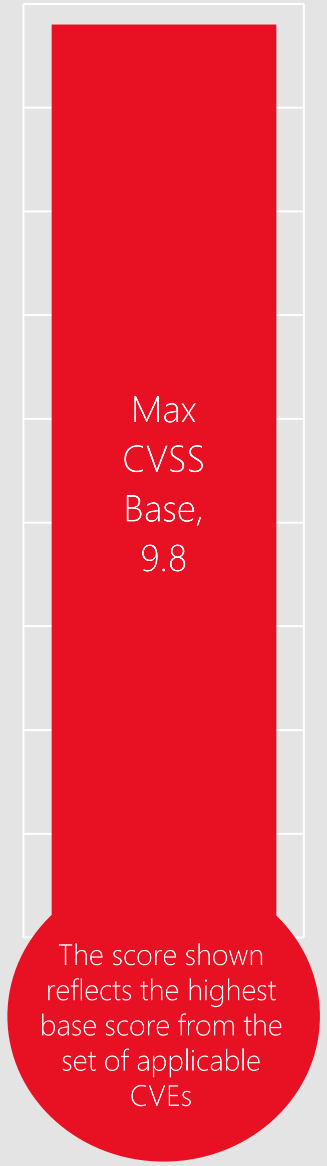


Windows 10 20H2 & Windows Server v20H2



Windows 10 1909

🟥 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:

Too many to list. Please see appendix for details.

CVE-2022-21901 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9 | Attack Vector: Adjacent | 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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Windows 8.1

CVE-2022-21850 Remote Desktop Client

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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1
Remote Desktop client
Windows Desktop

CVE-2022-21920 Kerberos

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
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-21874 Security Center API

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly 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.

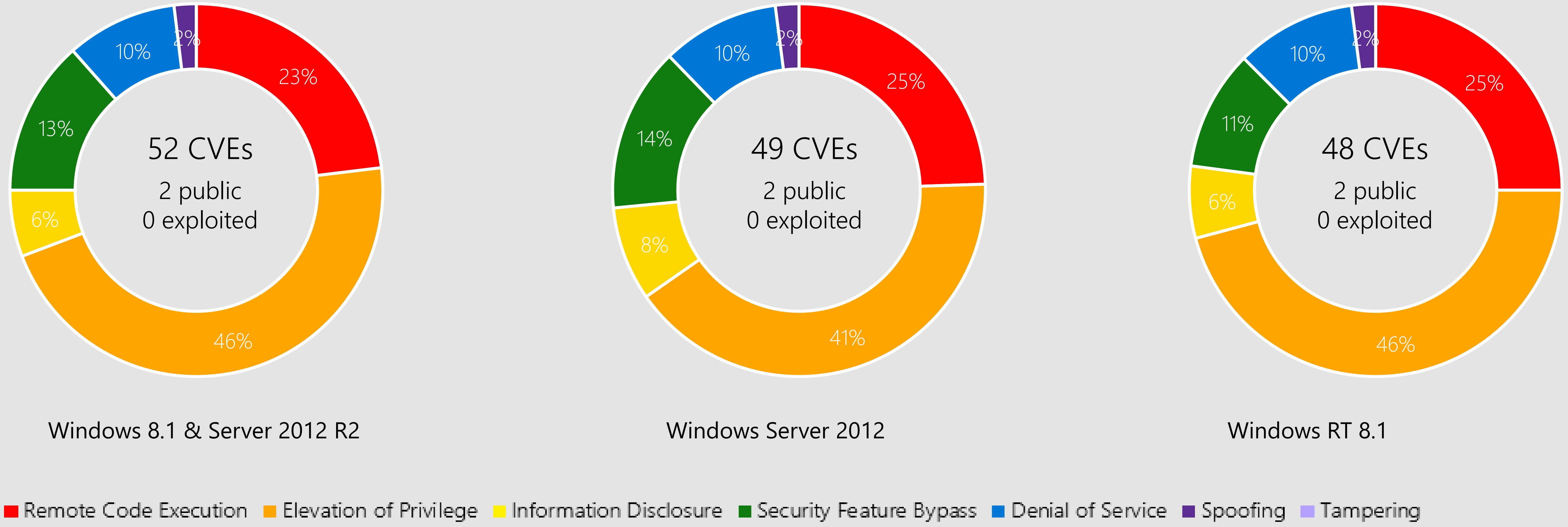
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016

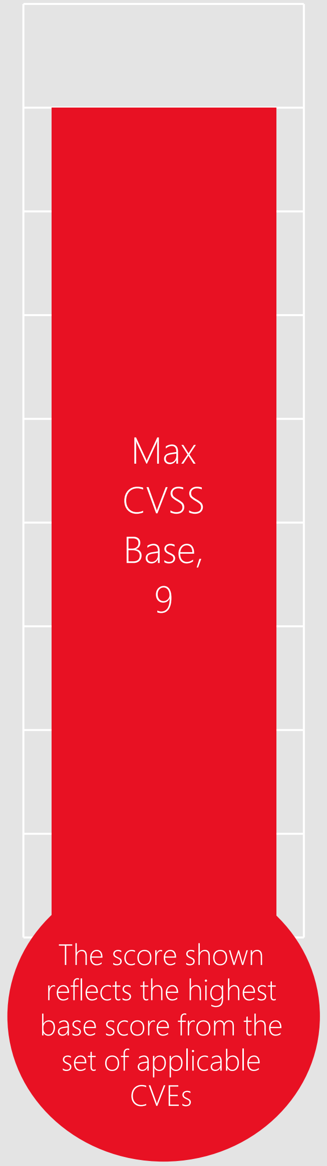
Windows 8.1, Server 2012 R2, and Server 2012



Windows 8.1 & Server 2012 R2

Windows Server 2012

Windows RT 8.1



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

Affected Components:

Too many to list. Please see appendix for details.

CVE-2022-21857 AD Domain 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

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-21836 Windows Certificates

Impact, Severity, Disclosure

Spoofing | Important | Publicly Disclosed | No known exploits in the wild

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

More Information

Link to security researcher article: https://eclypsium.com/2021/09/23/everyone-gets-a-rootkit/

Affected Software

Windows 11
Server 2022
Server, version 20H2
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2022-21919 User Profile Service

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7 | Attack Vector: Local | Attack Complexity: High | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

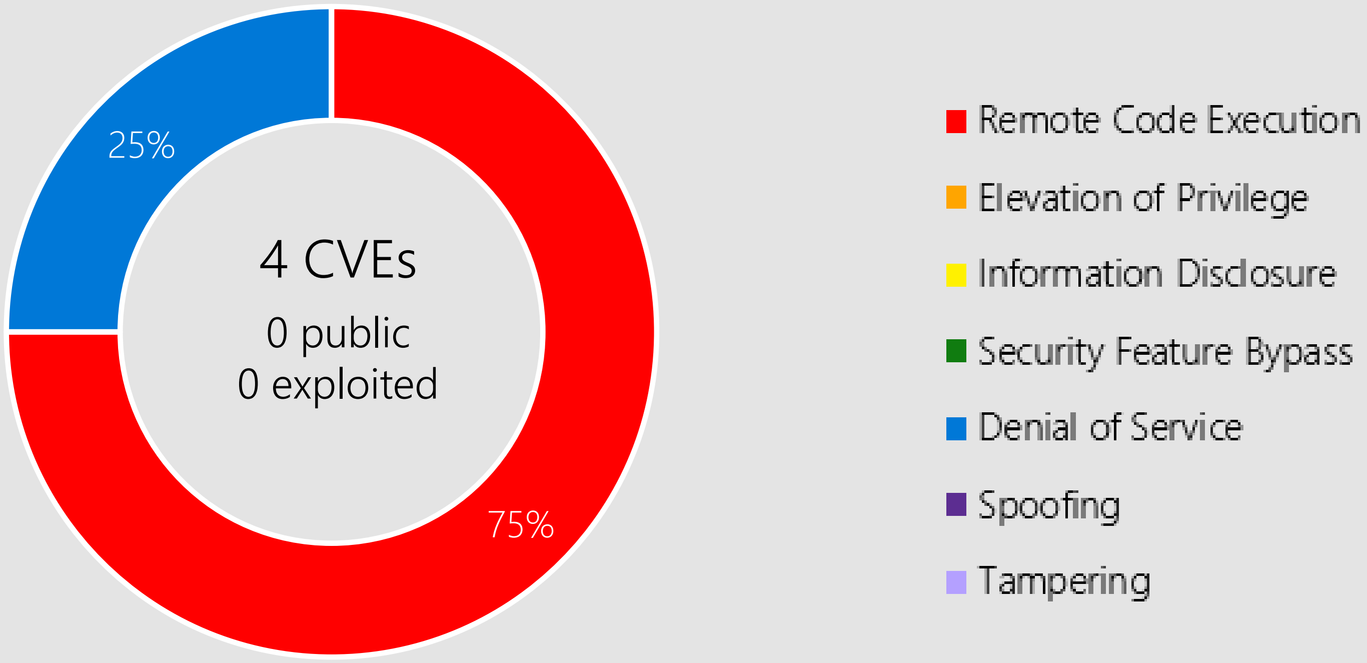
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Server 2022
Server, version 20H2
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
Word 2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Server Subscription Edition Language Pack

CVE-2022-21840 Office

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: 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

Excel 2013/2016
Office 2013/2016/2019
Office LTSC 2021
SharePoint Server —
Subscription Edition
SharePoint Server —
Sub Edition Language Pack
Office Web Apps Server 201
SharePoint Foundation 2013
SharePoint Server 2019
SharePoint Ent. Server 2016
SharePoint Ent. Server 2013
365 Apps Enterprise
Office LTSC for Mac 2021
Office 2019 for Mac
Office Online Server

CVE-2022-21837 SharePoint Server

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.3 | 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 Enterprise Server 2016
SharePoint Server 2019

Other Products

Exchange Server

CVE-2022-21846 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11.

CVE-2022-21855 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 21.

Other Products

Exchange Server

CVE-2022-21969 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 21.

Other Products

Dynamics 365

CVE-2022-21891 | 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 Sales.

CVE-2022-21932 | 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 Engagement V9.1, Dynamics 365 Customer Engagement V9.0.

Other Products

.NET Framework

CVE-2022-21911 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Framework 3.5, .NET Framework 3.5.1, .NET Framework 4.6, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2, .NET framework 4.6.2/4.7/4.7.1/4.7.2, .NET Framework 4.8

Other Products

Open Source

CVE-2021-36976 Libarchive

CVE-2021-22947 Curl

Security Advisory 170021 Office

What's Changed?

On 1/11/2022 Microsoft released an update for all supported versions of Excel that disables DDE Server Launch by default, protecting customers out of the box from attacks targeting DDE. DDE Server Launch can be enabled by setting the DisableDDEServerLaunch registry value to 0. Administrators can enable DDE Server Launch for Office 2016 and later by using the Group Policy template; administrators should be aware that users cannot disable DDE Server Launch if an administrator has enabled it via Group Policy. For more information see Microsoft Excel security enhancements in the January 2022 update.

Suggested Actions:

1. Apply the January Office updates
2. Evaluate any business need to re-enable DDE Server after carefully considering the security risks of doing so.

https://msrc.microsoft.com/update-guide/vulnerability/ADV170021

Product Lifecycle Update

Products reaching end of support in January

Visual Studio LightSwitch 2011

aka.ms/lifecycle

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-21852	No	No	DWM Core Library
CVE-2021-36976	Yes	No	Libarchive
CVE-2022-21919	Yes	No	User Profile Service
CVE-2022-21918	No	No	DirectX Graphics Kernel File
CVE-2022-21917	No	No	HEVC Video Extensions
CVE-2022-21915	No	No	GDI+
CVE-2022-21833	No	No	Virtual Machine IDE Drive
CVE-2022-21834	No	No	User-mode Driver Framework Reflector Driver
CVE-2022-21835	No	No	Cryptographic Services
CVE-2022-21836	Yes	No	Certificate
CVE-2022-21838	No	No	Cleanup Manager
CVE-2022-21839	Yes	No	Event Tracing Discretionary Access Control List
CVE-2022-21857	No	No	Active Directory Domain Services
CVE-2022-21858	No	No	Bind Filter Driver

CVE	Public	Exploited	Product
CVE-2022-21859	No	No	Accounts Control
CVE-2022-21860	No	No	AppContracts API Server
CVE-2022-21861	No	No	Task Flow Data Engine
CVE-2022-21862	No	No	Application Model Core API
CVE-2022-21863	No	No	StateRepository API Server file
CVE-2022-21864	No	No	UI Immersive Server API
CVE-2022-21865	No	No	Connected Devices Platform Service
CVE-2022-21866	No	No	System Launcher
CVE-2022-21867	No	No	Push Notifications Apps Elevation Of Privilege
CVE-2022-21868	No	No	Devices Human Interface
CVE-2022-21869	No	No	Clipboard User Service
CVE-2022-21870	No	No	Tablet User Interface Application Core
CVE-2022-21871	No	No	Diagnostics Hub Standard Collector Runtime
CVE-2022-21872	No	No	Event Tracing

CVE	Public	Exploited	Product
CVE-2022-21873	No	No	Tile Data Repository
CVE-2022-21874	Yes	No	Security Center API
CVE-2022-21875	No	No	Storage
CVE-2022-21876	No	No	Win32k
CVE-2022-21877	No	No	Storage Spaces Controller
CVE-2022-21878	No	No	Geolocation Service
CVE-2022-21879	No	No	Kernel
CVE-2022-21880	No	No	GDI+
CVE-2022-21881	No	No	Kernel
CVE-2022-21882	No	No	Win32k
CVE-2022-21843	No	No	IKE Extension
CVE-2022-21883	No	No	IKE Extension
CVE-2022-21884	No	No	Local Security Authority Subsystem Service
CVE-2022-21885	No	No	Remote Access Connection Manager

CVE	Public	Exploited	Product
CVE-2022-21887	No	No	Win32k
CVE-2022-21888	No	No	Modern Execution Server
CVE-2022-21892	No	No	Resilient File System (ReFS)
CVE-2022-21893	No	No	Remote Desktop Protocol
CVE-2022-21894	No	No	Secure Boot
CVE-2022-21900	No	No	Hyper-V
CVE-2022-21901	No	No	Hyper-V
CVE-2022-21902	No	No	DWM Core Library
CVE-2022-21903	No	No	GDI
CVE-2022-21904	No	No	GDI
CVE-2022-21905	No	No	Hyper-V
CVE-2022-21906	No	No	Defender Application Control
CVE-2022-21907	No	No	HTTP Protocol Stack
CVE-2022-21908	No	No	Installer

CVE	Public	Exploited	Product
CVE-2022-21910	No	No	Cluster Port Driver
CVE-2022-21912	No	No	DirectX Graphics Kernel
CVE-2022-21913	No	No	Local Security Authority (Domain Policy) Remote Protocol
CVE-2022-21924	No	No	Workstation Service Remote Protocol
CVE-2022-21925	No	No	BackupKey Remote Protocol
CVE-2022-21958	No	No	Resilient File System (ReFS)
CVE-2022-21959	No	No	Resilient File System (ReFS)
CVE-2022-21960	No	No	Resilient File System (ReFS)
CVE-2022-21961	No	No	Resilient File System (ReFS)
CVE-2022-21962	No	No	Resilient File System (ReFS)
CVE-2022-21963	No	No	Resilient File System (ReFS)
CVE-2022-21964	No	No	Remote Desktop Licensing Diagnoser
CVE-2022-22709	No	No	VP9 Video Extensions
CVE-2022-21847	No	No	Hyper-V

CVE	Public	Exploited	Product
CVE-2022-21922	No	No	Remote Procedure Call Runtime
CVE-2022-21921	No	No	Defender Credential Guard
CVE-2022-21920	No	No	Kerberos
CVE-2022-21848	No	No	IKE Extension
CVE-2022-21849	No	No	IKE Extension
CVE-2022-21850	No	No	Remote Desktop Client
CVE-2022-21851	No	No	Remote Desktop Client
CVE-2022-21916	No	No	Common Log File System Driver
CVE-2022-21895	No	No	User Profile Service
CVE-2022-21914	No	No	Remote Access Connection Manager
CVE-2022-21889	No	No	IKE Extension
CVE-2022-21890	No	No	IKE Extension
CVE-2022-21896	No	No	DWM Core Library
CVE-2022-21897	No	No	Common Log File System Driver

CVE	Public	Exploited	Product
CVE-2022-21898	No	No	DirectX Graphics Kernel
CVE-2022-21899	No	No	Extensible Firmware Interface
CVE-2022-21928	No	No	Resilient File System (ReFS)
CVE-2022-21929	No	No	Edge (Chromium-based)
CVE-2022-21930	No	No	Edge (Chromium-based)
CVE-2022-21931	No	No	Edge (Chromium-based)
CVE-2022-21954	No	No	Edge (Chromium-based)
CVE-2022-21970	No	No	Edge (Chromium-based)
CVE-2022-0096	No	No	Chromium
CVE-2022-0097	No	No	Chromium
CVE-2022-0098	No	No	Chromium
CVE-2022-0099	No	No	Chromium
CVE-2022-0100	No	No	Chromium
CVE-2022-0101	No	No	Chromium

CVE	Public	Exploited	Product
CVE-2022-0102	No	No	Chromium
CVE-2022-0103	No	No	Chromium
CVE-2022-0104	No	No	Chromium
CVE-2022-0105	No	No	Chromium
CVE-2022-0106	No	No	Chromium
CVE-2022-0107	No	No	Chromium
CVE-2022-0108	No	No	Chromium
CVE-2022-0109	No	No	Chromium
CVE-2022-0110	No	No	Chromium
CVE-2022-0111	No	No	Chromium
CVE-2022-0112	No	No	Chromium
CVE-2022-0113	No	No	Chromium
CVE-2022-0114	No	No	Chromium
CVE-2022-0115	No	No	Chromium

CVE	Public	Exploited	Product
CVE-2022-0116	No	No	Chromium
CVE-2022-0117	No	No	Chromium
CVE-2022-0118	No	No	Chromium
CVE-2022-0120	No	No	Chromium
CVE-2022-21840	No	No	Office
CVE-2022-21841	No	No	Excel
CVE-2022-21837	No	No	SharePoint Server
CVE-2022-21842	No	No	Word
CVE-2021-22947	Yes	No	Open Source Curl
CVE-2022-21932	No	No	Dynamics 365 Customer Engagement
CVE-2022-21911	No	No	.NET Framework
CVE-2022-21846	No	No	Exchange Server
CVE-2022-21855	No	No	Exchange Server

CVE	Public	Exploited	Product
CVE-2022-21891	No	No	Dynamics 365 (on-premises)
CVE-2022-21969	No	No	Exchange Server