Microsoft

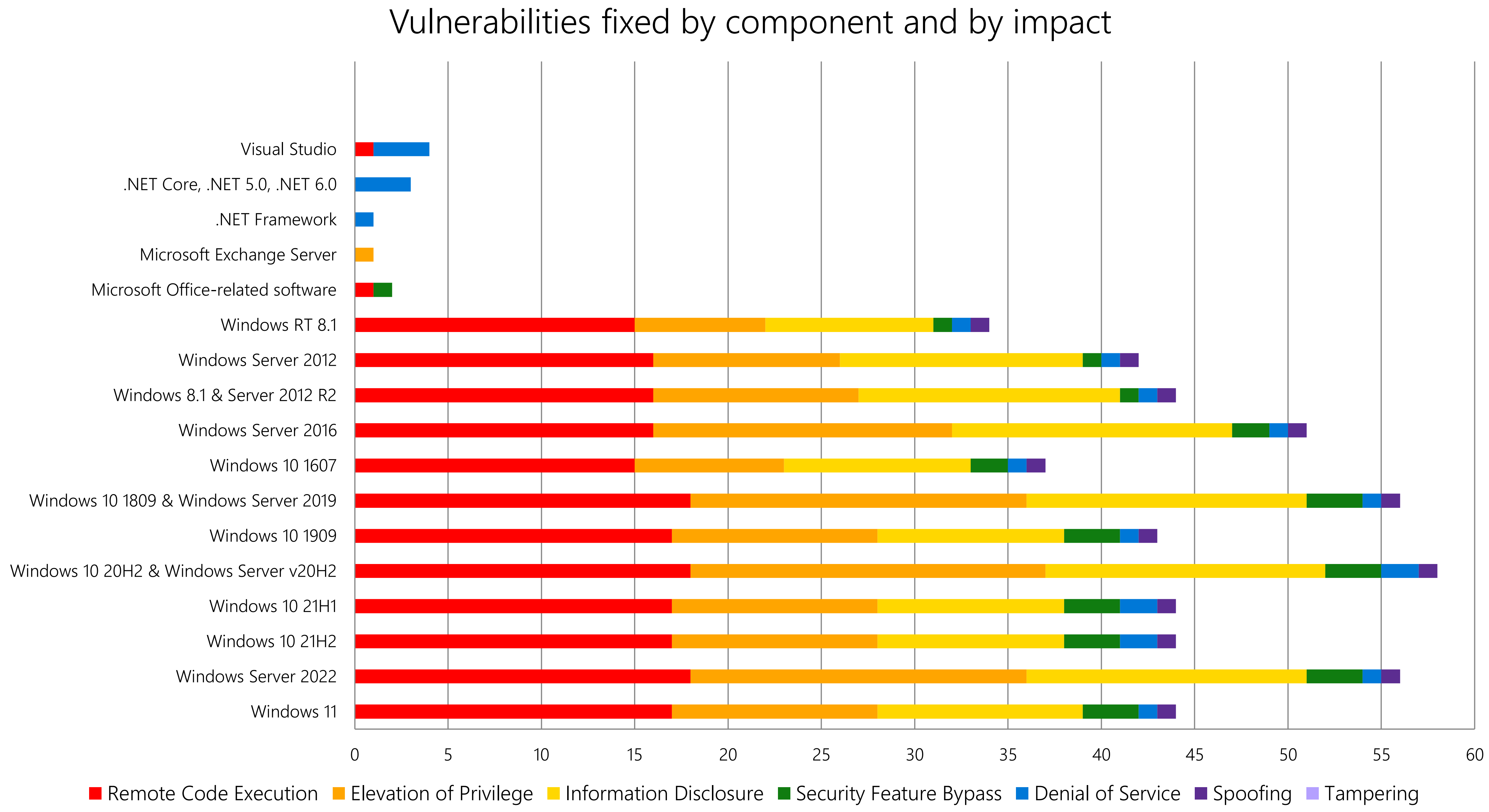
Microsoft Security Release

May 10, 2022

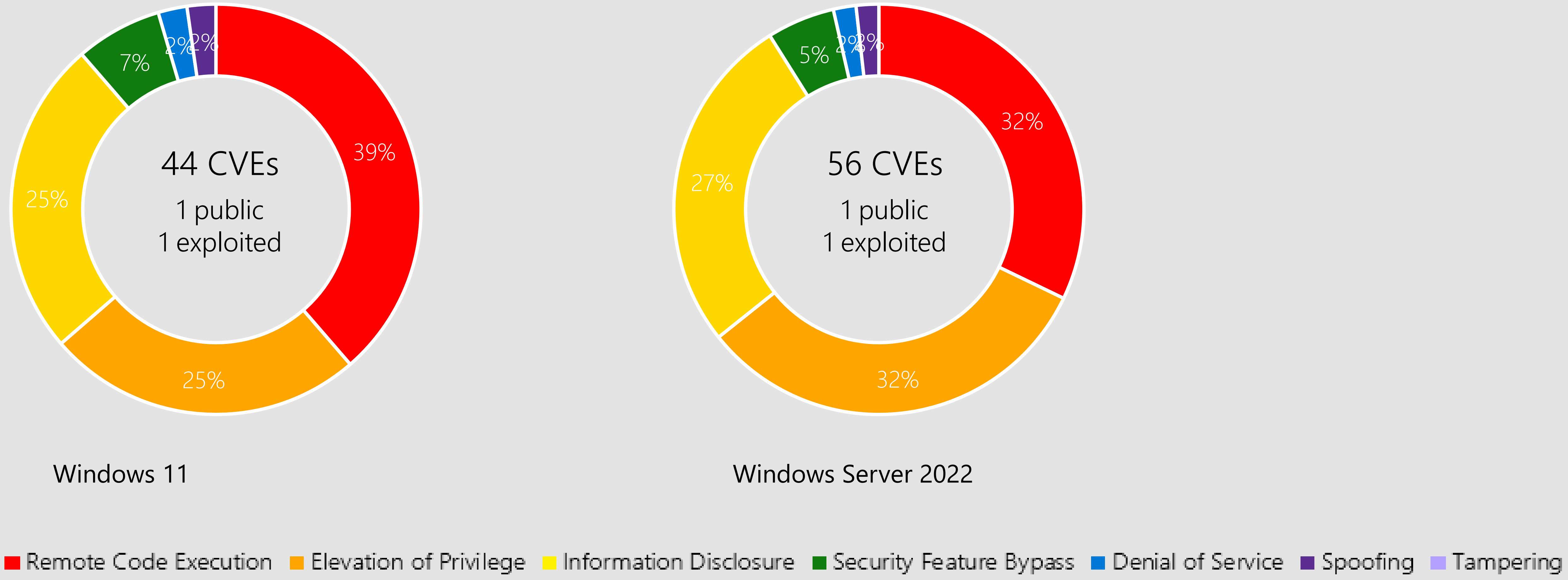
Agenda

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

Monthly Security Release Overview - May 2022

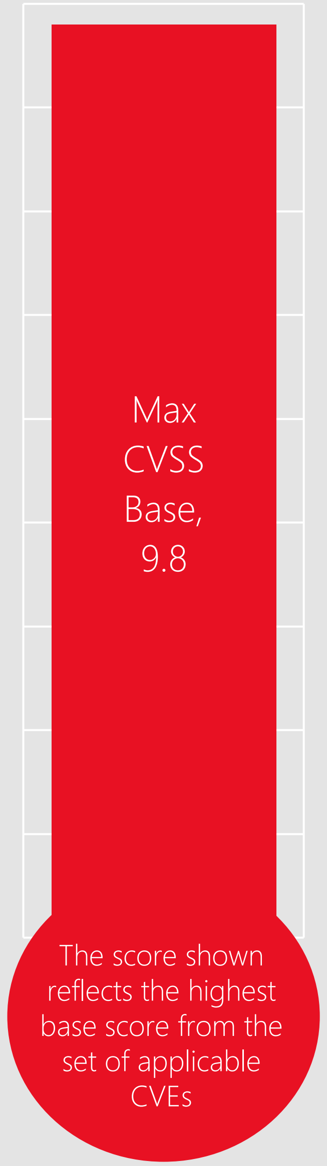


Windows 11, Server 2022



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:

Please see Appendix for complete list.

CVE-2022-26937 Network File System

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

Disable NFSV2 and NFSV3. See CVE entry for details.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2022
Server, version 20H2
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2022-22017 Remote Desktop Client

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.

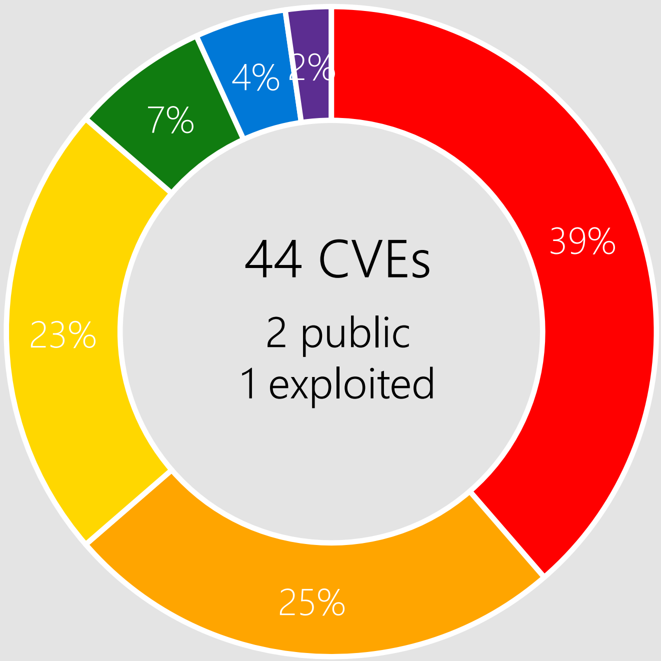
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

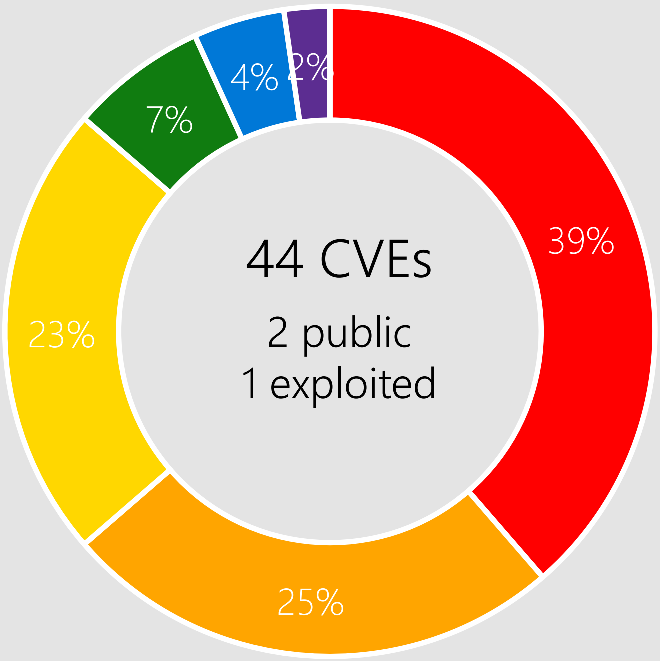
Affected Software

Windows 11
Server 2022
Remote Desktop Client for Windows Desktop

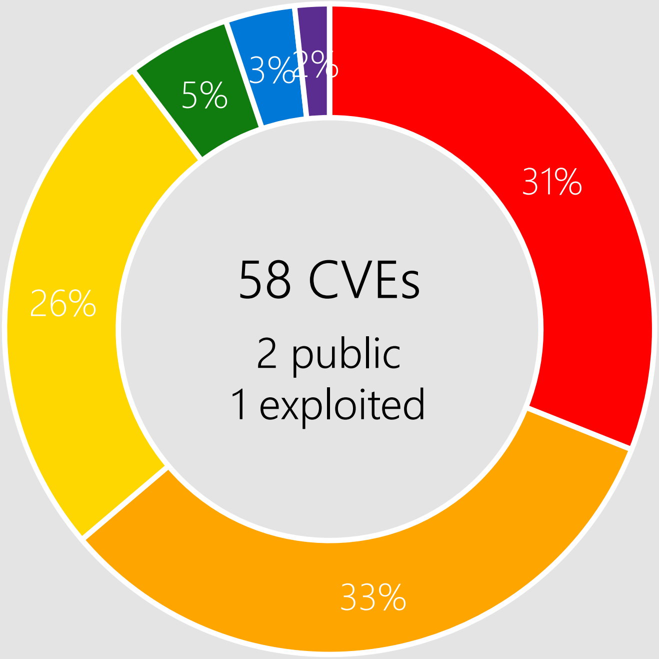
Windows 10



Windows 10 21H2

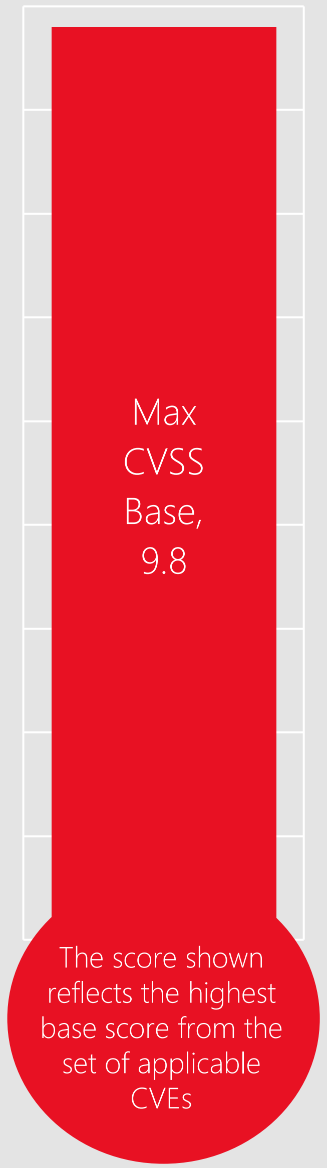


Windows 10 21H1



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-2022-22012 LDAP

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.

More Information

This vulnerability is only exploitable if the MaxReceiveBuffer LDAP policy is set to a value higher than the default value. See CVE entry for details.

Affected Software

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

CVE-2022-22019 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: 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-2022-26925 LSA

Impact, Severity, Disclosure

Spoofing | Important | Publicly Disclosed | Exploitation Detected

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.

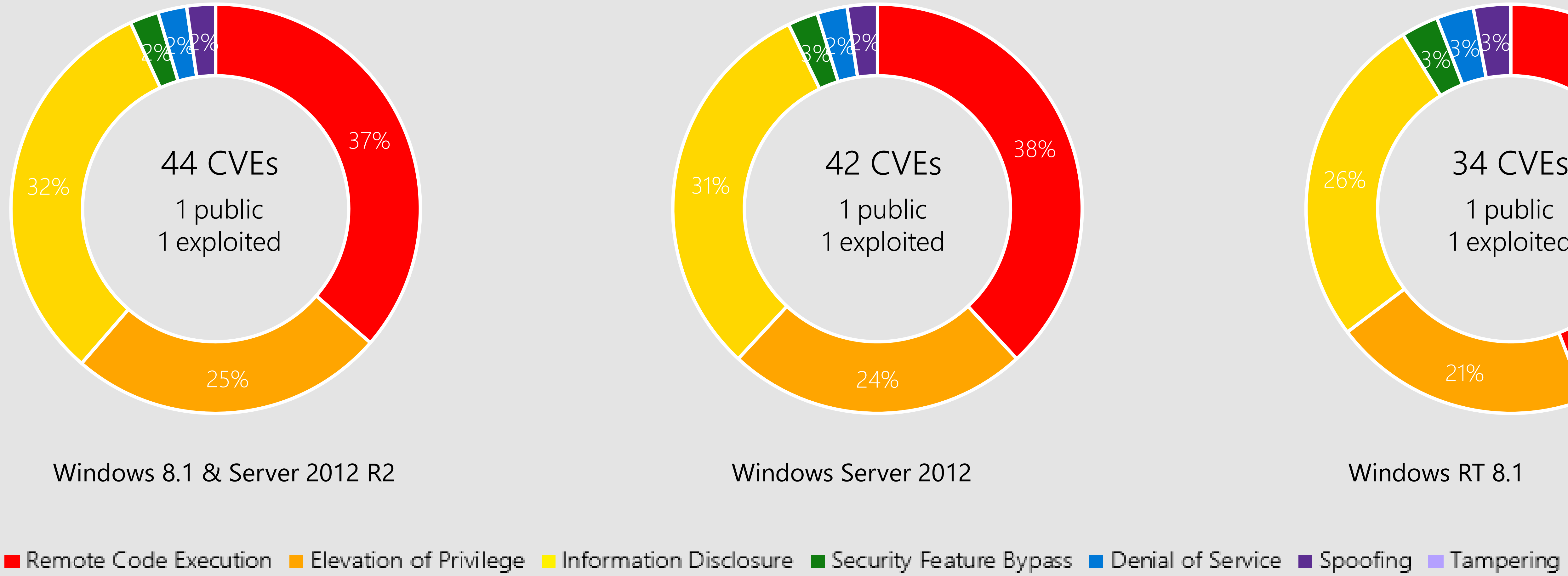
More Information

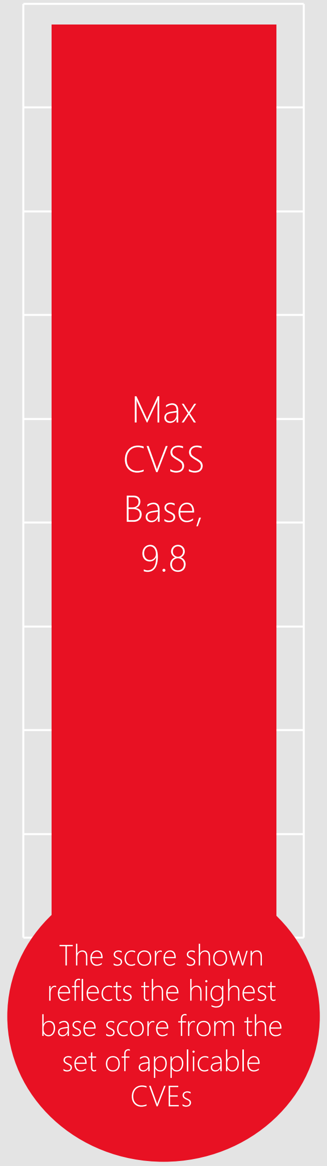
Recommendation: Mitigate NTLM relay attacks per ADV210003 and KB5005413

Affected Software

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

Windows 8.1, Server 2012 R2, and Server 2012




Max CVSS Base, 9.8

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

Affected Components:

Please see Appendix for complete list.

CVE-2022-26923 Active Directory 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

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

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-2022-21972 PPTP

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.

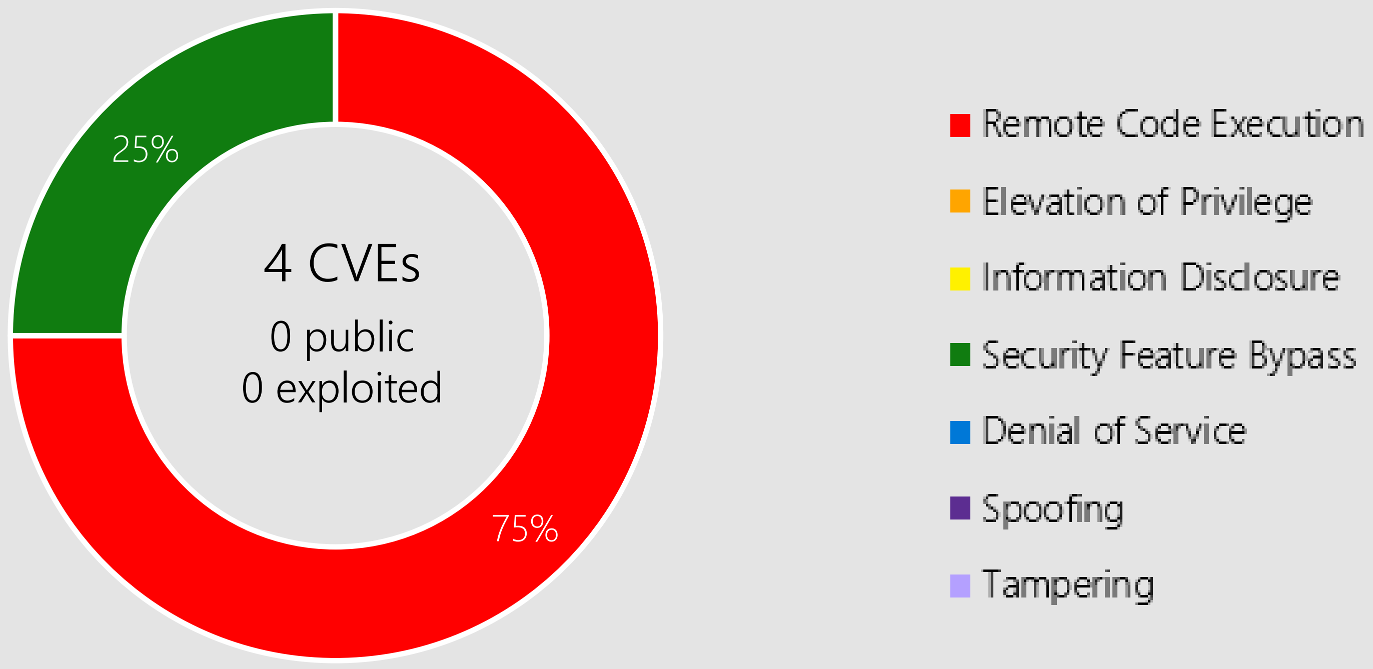
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
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 2019
Word 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
Publisher 2013
Publisher 2016
SharePoint Foundation 2013
SharePoint Server Subscription Edition

CVE-2022-29108 SharePoint Server

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

SharePoint Server Subscription Edition

SharePoint Foundation 2013

SharePoint Enterprise Server 2016

SharePoint Server 2019

CVE-2022-29109 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

365 Apps Enterprise
Office LTSC 2021
Office 2019
Office Online Server

Other Products

Exchange Server

CVE-2022-21978 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.2
Attack Vector: Local
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11.

Note: additional steps required to deploy May security update. Install May SU, then run "Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAllDomains"
More Information: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-may-2022-exchange-server-security-updates/ba-p/3301831

Other Products

.NET 5.0, .NET 6.0, .NET Core

CVE-2022-23267 | 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 Core 3.1, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0, .NET 6.0.

CVE-2022-29117 | 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 Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, .NET 5.0, .NET 6.0.

Other Products

.NET 5.0, .NET 6.0, .NET Core

CVE-2022-29145 | 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 Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.1, .NET 5.0, .NET 6.0.

Other Products

.NET Framework

CVE-2022-30130 | Low | Denial of Service | Public: No | Exploited: No

CVSS Base Score 3.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET Framework 3.5 AND 4.8 on relevant Windows versions, .NET Framework 3.5 AND 4.7.2 on relevant Windows versions, .NET Framework 4.8 on relevant Windows versions, .NET Framework 3.5, .NET Framework 3.0 on relevant Windows versions, .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on relevant Windows versions, .NET Framework 2.0 on relevant Windows versions, .NET Framework 4.6 on relevant Windows versions, .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on relevant Windows versions, .NET Framework 3.5.1. on relevant Windows versions.

Other Products

Visual Studio

CVE-2022-29148 | 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 2017 version 15.9 (includes 15.0 - 15.8).

CVE-2022-29145 | 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 Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.1, .NET 5.0, .NET 6.0.

Other Products

Visual Studio

CVE-2022-23267 | 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 Core 3.1, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0, .NET 6.0.

CVE-2022-29117 | 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 Core 3.1, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 version 17.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, .NET 5.0, .NET 6.0.

Other Products

Visual Studio

CVE-2022-30129 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio Code.

Other Products

Self-hosted Integration Runtime

CVE-2022-29972 | Critical | Remote Code Execution | Public: Yes | Exploited: No

- CVSS Score: The vulnerability in the Redshift driver referenced in the CVE impacts Microsoft services listed in the affected software table. The environmental score as it relates to affected Microsoft services can be different than the score assigned by the owner of the CVE. The base environmental score that Microsoft has assigned is 8.2

Security Advisory ADV220001

Overview

Microsoft recently mitigated and remediated a vulnerability affecting Azure Data Factory and Azure Synapse Pipelines. The vulnerability was found in the third-party ODBC data connector used to connect to Amazon Redshift, in Integration Runtime (IR) in Azure Synapse Pipelines, and Azure Data Factory. The vulnerability could have allowed an attacker to execute remote commands across Integration Runtimes.

We addressed the vulnerability with the release of the security updates to remediate CVE-20220-29972. In addition, we also worked with the third-party vendor on fixing the vulnerability in the driver which has been released with our latest updates. More information can be found on our blog.

Suggested Actions:

No customer action is expected for this change. However, in the event customers must perform an action in response to these changes, they will be notified via Azure Service Health Alerts.

ADV220001 - Security Update Guide - Microsoft - Upcoming improvements to Azure Data Factory and Azure Synapse Pipeline infrastructure in response to CVE-2022-29972

Product Lifecycle Update

Windows 10 Semi-Annual Channel end of service

Windows 10 Ent & EDU 1909
Windows 10 Home & Pro 20H2

aka.ms/lifecycle

[Windows Lifecycle FAQ]

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5014025	May 2022
Windows Server 2012	5014027	May 2022
Windows 10 1607/Server 2016	5014026	May 2022
Windows 10 1809/Server 2019	5005112	August 2021
Windows 10 1909	5005412	August 2021
Windows 10 2004/Windows Server, version 2004	5005260	August 2021
Windows 10 20H2/Windows Server, version 20H2	5005260	August 2021
Windows 10 21H1	5005260	August 2021

4. Why have the 2004, 20H2, and 21H1 rows been added back to the table for the August 2021 updates?
For Windows Server Update Services (WSUS) deployment or when installing the standalone package from Microsoft Update Catalog:
If your devices do not have the May 11, 2021 update (KB5003173) or later LCU, you **must** install the special standalone August 10, 2021 SSU (KB5005260).

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-21972	No	No	Point-to-Point Tunneling Protocol
CVE-2022-22713	Yes	No	Hyper-V
CVE-2022-23270	No	No	Point-to-Point Tunneling Protocol
CVE-2022-24466	No	No	Hyper-V
CVE-2022-26913	No	No	Authentication
CVE-2022-26925	Yes	Yes	LSA
CVE-2022-26926	No	No	Address Book
CVE-2022-26927	No	No	Graphics Component
CVE-2022-26930	No	No	Remote Access Connection Manager
CVE-2022-26931	No	No	Kerberos
CVE-2022-26932	No	No	Storage Spaces Direct
CVE-2022-26933	No	No	NTFS
CVE-2022-26934	No	No	Graphics Component
CVE-2022-26935	No	No	WLAN AutoConfig Service

CVE	Public	Exploited	Product
CVE-2022-26936	No	No	Server Service
CVE-2022-26937	No	No	Network File System
CVE-2022-26938	No	No	Storage Spaces Direct
CVE-2022-26939	No	No	Storage Spaces Direct
CVE-2022-22011	No	No	Graphics Component
CVE-2022-22012	No	No	LDAP
CVE-2022-22013	No	No	LDAP
CVE-2022-22014	No	No	LDAP
CVE-2022-22015	No	No	Remote Desktop Protocol (RDP)
CVE-2022-22016	No	No	PlayToManager
CVE-2022-29102	No	No	Failover Cluster
CVE-2022-29103	No	No	Remote Access Connection Manager
CVE-2022-29104	No	No	Print Spooler
CVE-2022-29105	No	No	Media Foundation

CVE	Public	Exploited	Product
CVE-2022-29106	No	No	Hyper-V Shared Virtual Disk
CVE-2022-29112	No	No	Graphics Component
CVE-2022-29113	No	No	Digital Media Receiver
CVE-2022-29114	No	No	Print Spooler
CVE-2022-29115	No	No	Fax Service
CVE-2022-29125	No	No	Push Notifications Apps
CVE-2022-29126	No	No	Tablet User Interface Application Core
CVE-2022-29127	No	No	BitLocker
CVE-2022-29128	No	No	LDAP
CVE-2022-29129	No	No	LDAP
CVE-2022-29130	No	No	LDAP
CVE-2022-29131	No	No	LDAP
CVE-2022-29132	No	No	Print Spooler
CVE-2022-29133	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2022-29134	No	No	Clustered Shared Volume
CVE-2022-29135	No	No	Cluster Shared Volume (CSV)
CVE-2022-29137	No	No	LDAP
CVE-2022-29138	No	No	Clustered Shared Volume
CVE-2022-29139	No	No	LDAP
CVE-2022-29140	No	No	Print Spooler
CVE-2022-29141	No	No	LDAP
CVE-2022-29142	No	No	Kernel
CVE-2022-22019	No	No	Remote Procedure Call Runtime
CVE-2022-23279	No	No	ALPC
CVE-2022-26923	No	No	Active Directory Domain Services
CVE-2022-29116	No	No	Kernel
CVE-2022-29120	No	No	Clustered Shared Volume
CVE-2022-29121	No	No	WLAN AutoConfig Service

CVE	Public	Exploited	Product
CVE-2022-29122	No	No	Clustered Shared Volume
CVE-2022-29123	No	No	Clustered Shared Volume
CVE-2022-29150	No	No	Cluster Shared Volume (CSV)
CVE-2022-29151	No	No	Cluster Shared Volume (CSV)
CVE-2022-26905	No	No	Edge (Chromium-based)
CVE-2022-29107	No	No	Office
CVE-2022-29108	No	No	SharePoint Server
CVE-2022-29109	No	No	Excel
CVE-2022-29110	No	No	Excel
CVE-2022-21978	No	No	Exchange Server
CVE-2022-23267	No	No	.NET and Visual Studio
CVE-2022-26940	No	No	Remote Desktop Protocol Client
CVE-2022-22017	No	No	Remote Desktop Client
CVE-2022-29117	No	No	.NET and Visual Studio

CVE	Public	Exploited	Product
CVE-2022-29145	No	No	.NET and Visual Studio
CVE-2022-29148	No	No	Visual Studio
CVE-2022-29972	Yes	No	Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver
CVE-2022-30130	No	No	
ADV220001	No	No	
CVE-2022-30129	No	No	