Microsoft

Microsoft Security Release

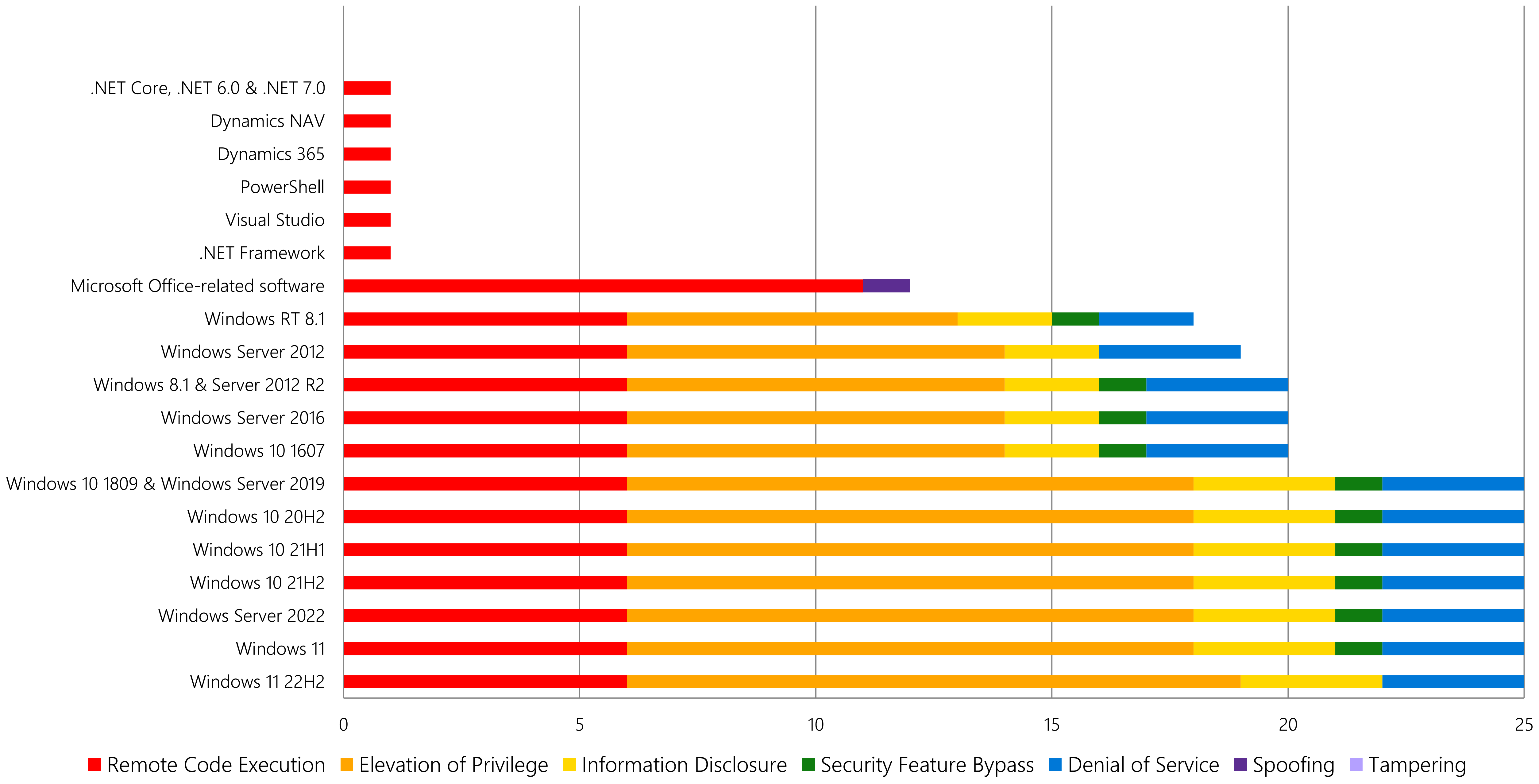
December 13, 2022

Agenda

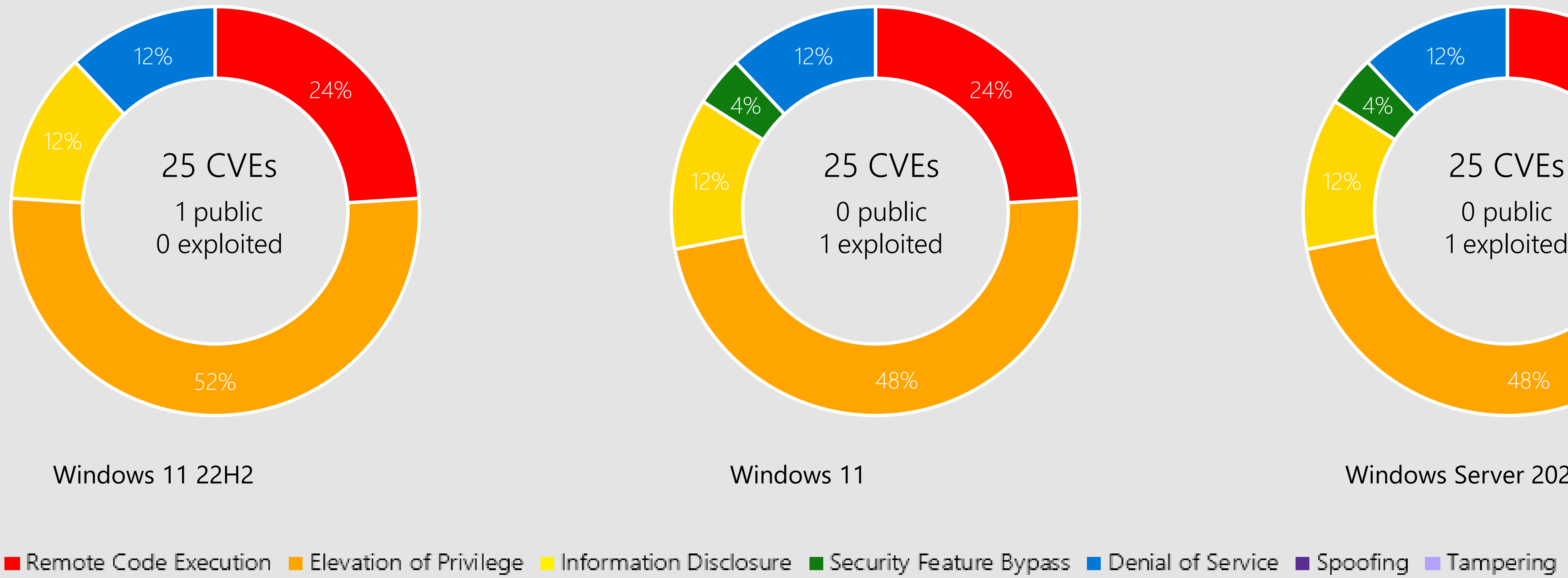
- Security Updates
- Security Advisory
- Product Support Lifecyle
- Other resources related to the release

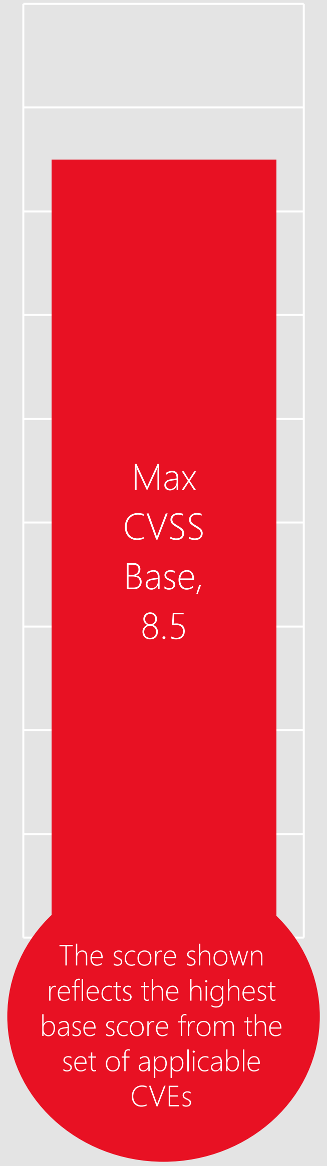
Monthly Security Release Overview - December 2022

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
- Contacts
- Error Reporting
- Fax Compose Form
- Graphics Component
- Hyper-V
- Kernel
- Media
- PowerShell
- Print Spooler
- Projected File System
- Secure Socket Tunneling Protocol (SSTP)
- SmartScreen
- Subsystem for Linux (WSL2) Kernel

CVE-2022-44710 DirectX Graphics Kernel

Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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

CVE-2022-41076 PowerShell

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.5 | Attack Vector: Network | Attack Complexity: High | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

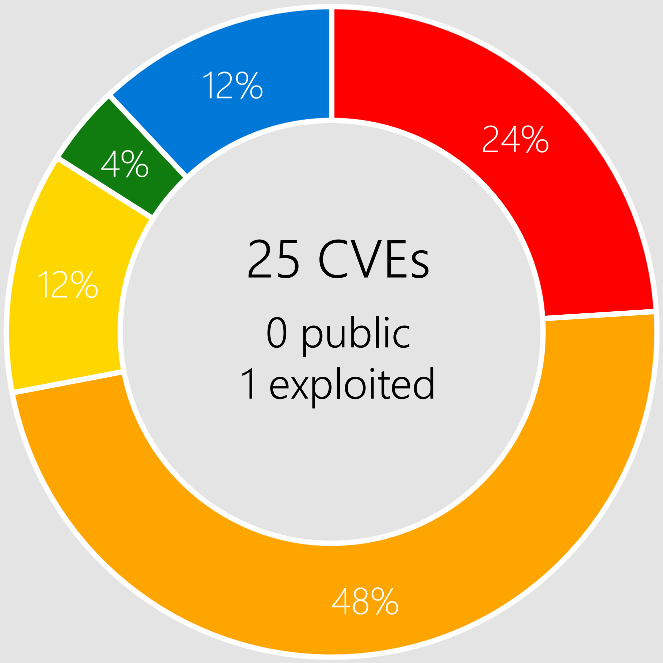
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

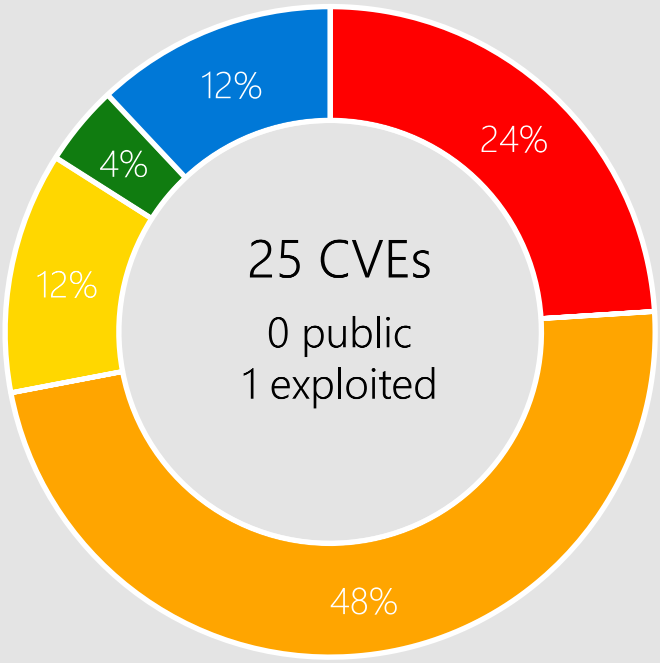
Windows 11 22H2
Windows 11
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1
PowerShell 7.2
PowerShell 7.3

Windows 10



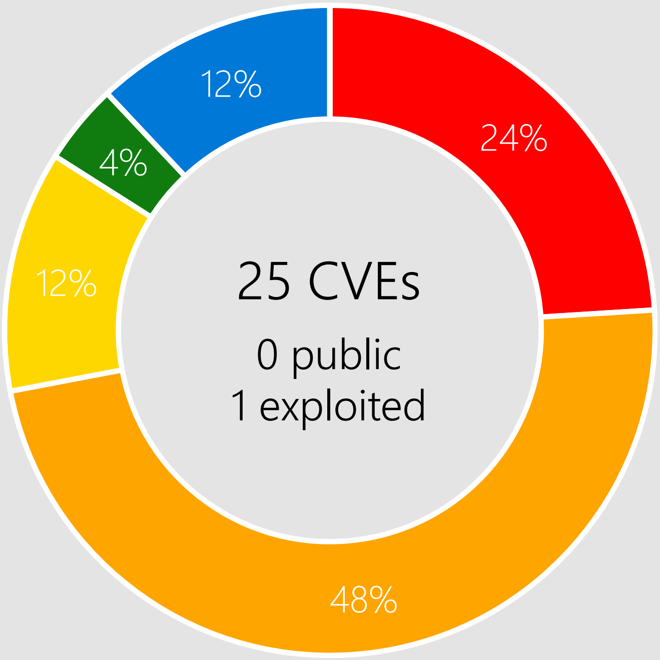
25 CVEs
0 public
1 exploited

Windows 10 21H2



25 CVEs
0 public
1 exploited

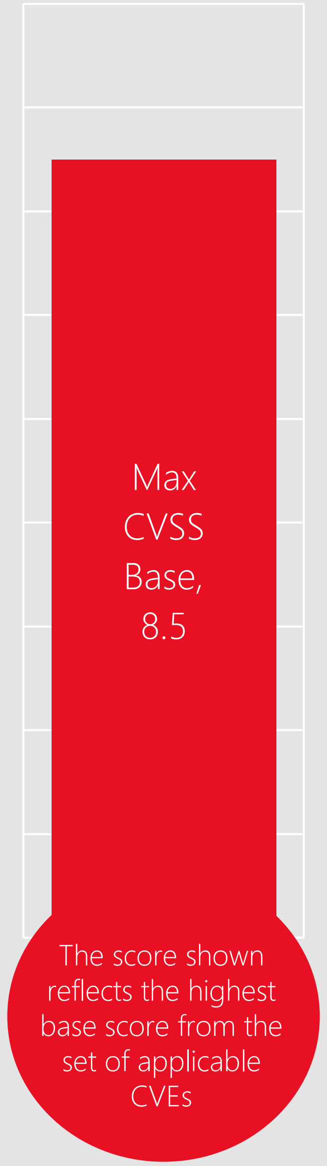
Windows 10 21H1



25 CVEs
0 public
1 exploited

Windows 10 20H2 & Windows Server v20H2

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



Max CVSS Base, 8.5

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

Affected Components:

Bluetooth Driver
Contacts
Error Reporting
Fax Compose Form

Graphics Component
Hyper-V
Kernel

Media
PowerShell
Print Spooler

Projected File System
Secure Socket Tunneling Protocol (SSTP)

SmartScreen
Subsystem for Linux (WSL2) Kernel

CVE-2022-44698 MOTW

Impact, Severity, Disclosure

Security Feature Bypass | Moderate | Privately disclosed | Exploits in the wild

CVSSScoreMetrics

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

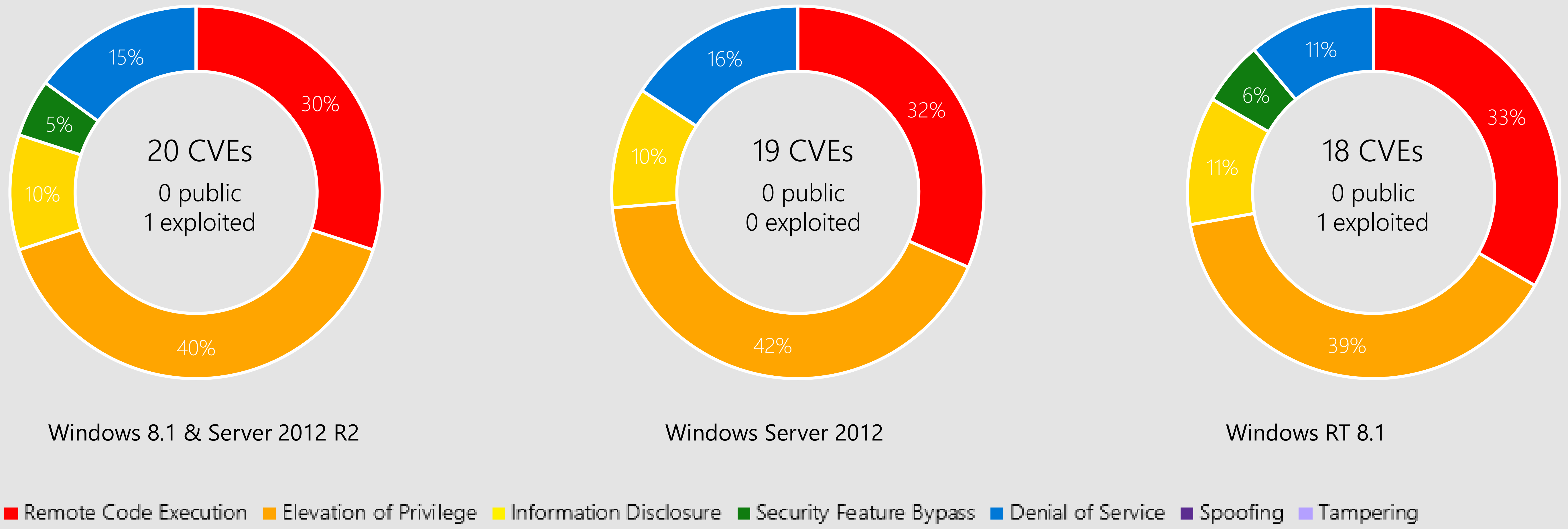
More Information

When you download a file from the internet, Windows adds the zone identifier or Mark of the Web as an NTFS stream to the file. So, when you run the file, Windows SmartScreen checks if there is a zone identifier Alternate Data Stream (ADS) attached to the file. If the ADS indicates ZoneId=3 which means that the file was downloaded from the internet, the SmartScreen does a reputation check.

Affected Software

Windows 11
Server 2022
Server 2019
Windows 10
Server 2016

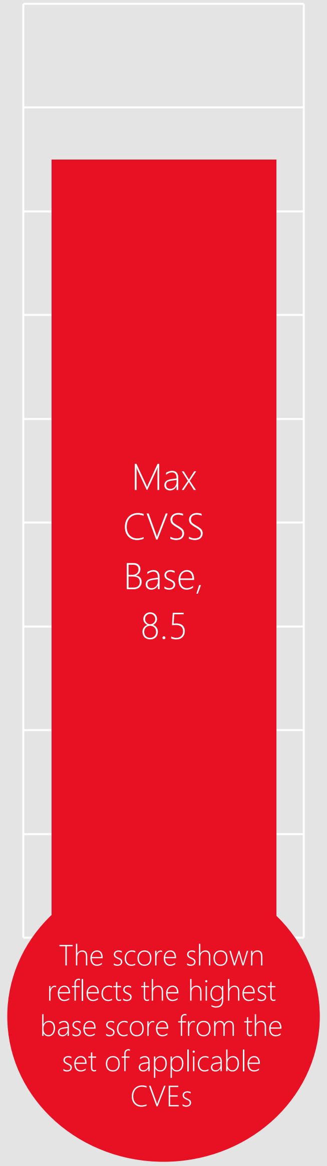
Windows 8.1, Server 2012 R2, and Server 2012



Windows 8.1 & Server 2012 R2

Windows Server 2012

Windows RT 8.1



Max CVSS Base, 8.5

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

Affected Components:

Bluetooth Driver
Contacts
Fax Compose Form

Graphics Component
Hyper-V
Kernel

Media
PowerShell
Print Spooler

Secure Socket Tunneling Protocol (SSTP)
SmartScreen

CVE-2022-44676 Secure Socket Tunneling Protocol (SSTP)

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.

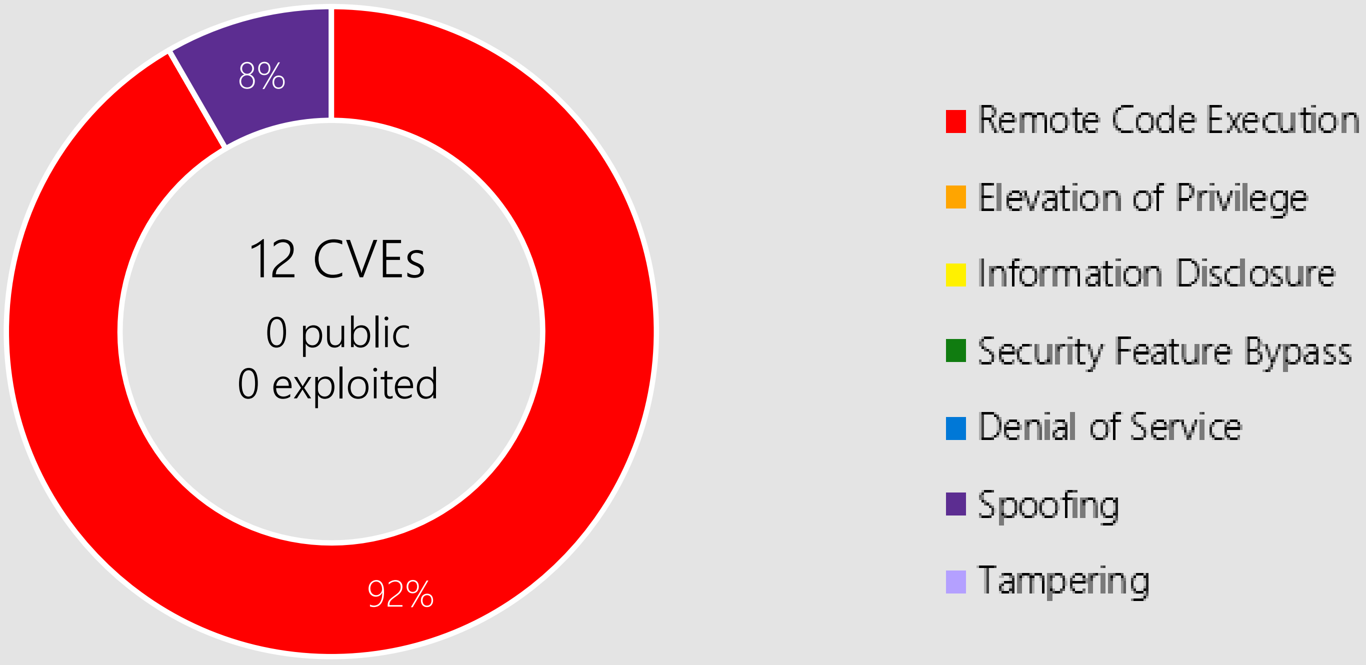
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

Microsoft Office



Microsoft Office-related software

Products:

Office 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
Visio 2013
Visio 2016

CVE-2022-44690 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-2022-44692 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 for Mac

Other Products

Dynamics 365 Business Central

CVE-2022-41127 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 Business Central 2020 Release Wave 1, Dynamics 365 Business Central 2021 Release Wave 1, Dynamics 365 Business Central 2022 Release Wave 1, Dynamics 365 Business Central 2022 Release Wave 2, Dynamics 365 Business Central 2021 Release Wave 2, Dynamics 365 Business Central 2020 Release Wave 2, Dynamics 365 Business Central Spring 2019 Update, Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)

Other Products

Dynamics NAV

CVE-2022-41127 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Dynamics NAV 2016, Dynamics NAV 2018, Dynamics NAV 2017.

Other Products

.NET Core, .NET 6.0, NET 7.0

CVE-2022-41089 | 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: .NET Core 3.1, .NET 6.0, .NET 7.0.

Other Products

.NET Framework

CVE-2022-41089 | 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: See CVE entry for a full list of .NET Framework versions

Other Products

Visual Studio

CVE-2022-41089 | 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 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.4

Other Products

Azure, Store Apps, and Windows Utilities

CVE-2022-44699 Azure Network Watcher VM Extension
CVE-2022-44704 Windows Sysmon
CVE-2022-44702 Windows Terminal
CVE-2022-24480 Outlook for Android

Security Advisory 220005 Microsoft Signed Drivers Used Maliciously

Summary

Microsoft was recently informed that drivers certified by Microsoft's Windows Hardware Developer Program were being used maliciously in post-exploitation activity. Microsoft has completed its investigation and determined that the activity was limited to the abuse of several developer program accounts and that no compromise has been identified. We've suspended the partners' seller accounts and implemented blocking detections 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.

ADV220005 - Security Update Guide - Microsoft - Guidance on Microsoft Signed Drivers Being Used Maliciously

Product Lifecycle Update

End of Support Products- Nothing in December

January 2023
Windows 8.1

Release End of Servicing

Windows 10, version 21H1
NET Core 3.1

aka.ms/lifecycle

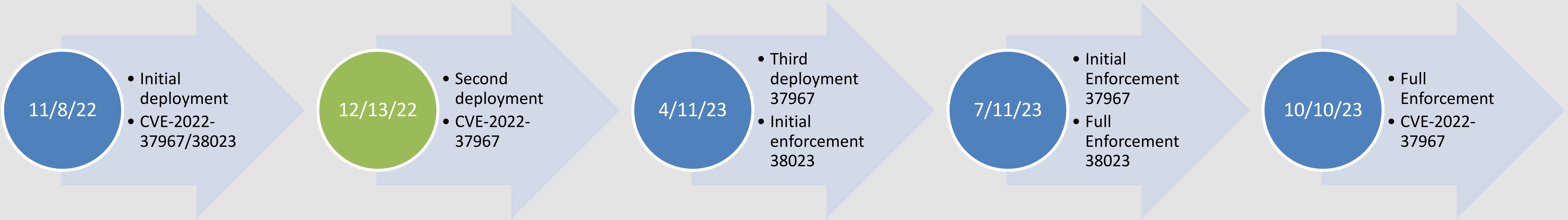
Latest Servicing Stack Updates

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
- Third deployment 37967
- 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

Microsoft

Questions?

Appendix

Known Issue: Server 2022 and Server 2019

System Center VMM might have issues using new NICs with VMs

After installing KB5021249 on Hyper-V hosts managed by System Center Virtual Machine Manager (VMM), you might receive an error on workflows involving creating a new Network Adapter (also called Network Interface Card or NIC) joined to a VM network or a new Virtual Machine (VM) with a Network Adapter joined to a VM network. Existing VMs with existing Network Adapters should not have issues connecting after installing KB5021249, only new Network Adapters created after installation of KB5021249 are affected.

Identifying the Issue and Workarounds

See the complete description of the issue in the Known Issues section of Windows Release Health:

Server 2022 WRH: Windows Server 2022 | Microsoft Learn

Server 2019 WRH: Windows 10, version 1809 and Windows Server 2019 | Microsoft Learn

CVE	Public	Exploited	Product
CVE-2022-44666	No	No	Contacts
CVE-2022-44667	No	No	Media
CVE-2022-44668	No	No	Media
CVE-2022-44673	No	No	Client Server Run-Time Subsystem (CSRSS)
CVE-2022-44674	No	No	Bluetooth Driver
CVE-2022-44675	No	No	Bluetooth Driver
CVE-2022-44676	No	No	Secure Socket Tunneling Protocol (SSTP)
CVE-2022-44677	No	No	Projected File System
CVE-2022-44678	No	No	Print Spooler
CVE-2022-44679	No	No	Graphics Component
CVE-2022-44680	No	No	Graphics Component
CVE-2022-44681	No	No	Print Spooler
CVE-2022-44682	No	No	Hyper-V
CVE-2022-44683	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2022-44692	No	No	Office Graphics
CVE-2022-44697	No	No	Graphics Component
ADV220005	No	No	Guidance on Signed Drivers Being Used Maliciously
CVE-2022-44698	No	Yes	SmartScreen
CVE-2022-44702	No	No	Terminal
CVE-2022-44704	No	No	Sysmon
CVE-2022-44707	No	No	Kernel
CVE-2022-41094	No	No	Hyper-V
CVE-2022-41074	No	No	Graphics Component
CVE-2022-41076	No	No	PowerShell
CVE-2022-41077	No	No	Fax Compose Form
CVE-2022-41121	No	No	Graphics Component
CVE-2022-44669	No	No	Error Reporting
CVE-2022-44670	No	No	Secure Socket Tunneling Protocol (SSTP)

CVE	Public	Exploited	Product
CVE-2022-44671	No	No	Graphics Component
CVE-2022-44687	No	No	Raw Image Extension
CVE-2022-44689	No	No	Subsystem for Linux (WSL2) Kernel
CVE-2022-44710	Yes	No	DirectX Graphics Kernel
CVE-2022-44688	No	No	Edge (Chromium-based)
CVE-2022-44708	No	No	Edge (Chromium-based)
CVE-2022-41115	No	No	Edge (Chromium-based) Update
CVE-2022-44690	No	No	SharePoint Server
CVE-2022-44691	No	No	Office OneNote
CVE-2022-44693	No	No	SharePoint Server
CVE-2022-44694	No	No	Office Visio
CVE-2022-44695	No	No	Office Visio
CVE-2022-44696	No	No	Office Visio
CVE-2022-44713	No	No	Outlook for Mac

CVE	Public	Exploited	Product
CVE-2022-41127	No	No	Dynamics NAV and Dynamics 365 Business Central (On Premises)
CVE-2022-41089	No	No	.NET Framework
CVE-2022-44699	No	No	Azure Network Watcher Agent
CVE-2022-26804	No	No	Office Graphics
CVE-2022-26805	No	No	Office Graphics
CVE-2022-26806	No	No	Office Graphics
CVE-2022-47211	No	No	Office Graphics
CVE-2022-47212	No	No	Office Graphics
CVE-2022-47213	No	No	Office Graphics