Microsoft

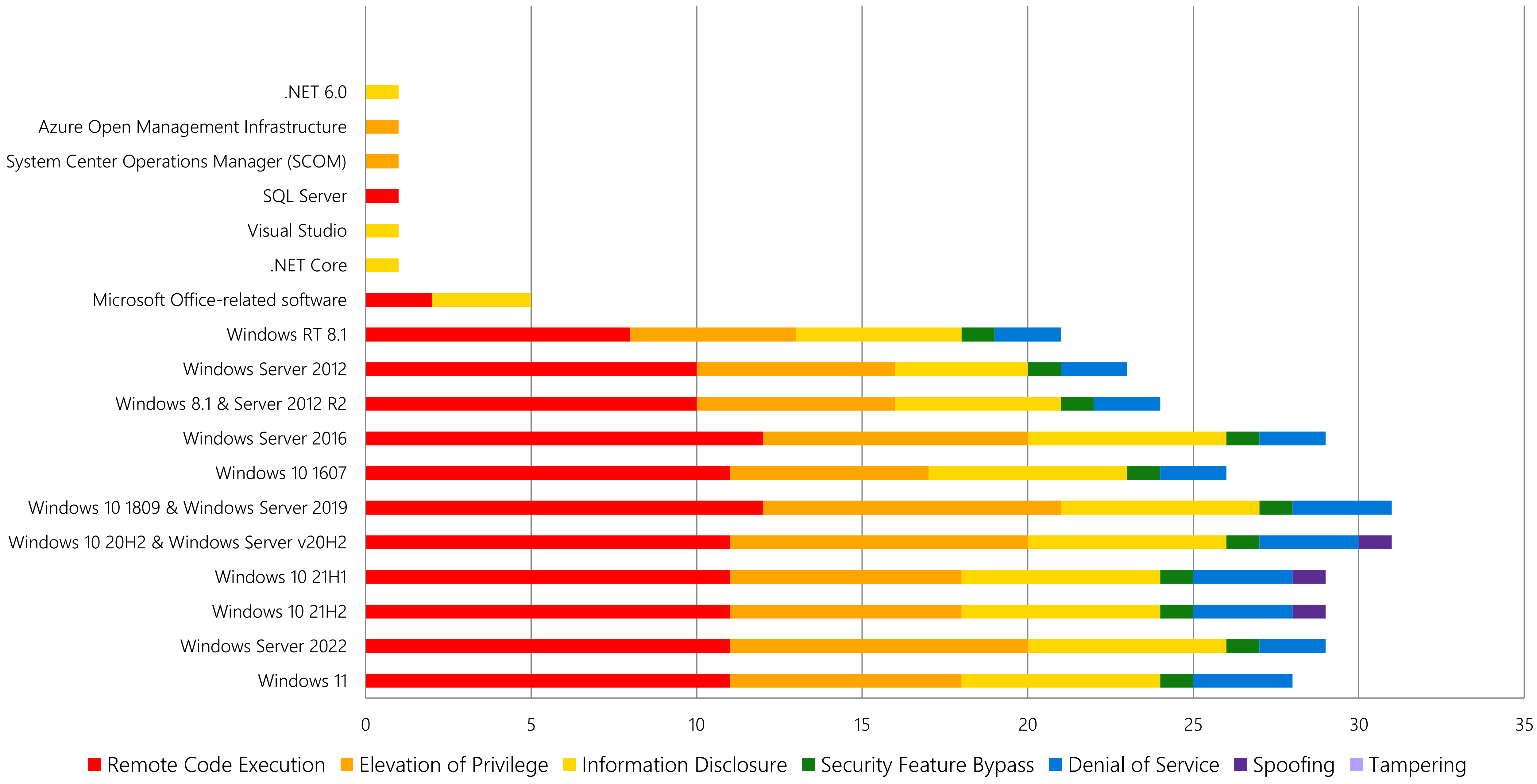
Microsoft Security Release

June 14, 2022

Agenda

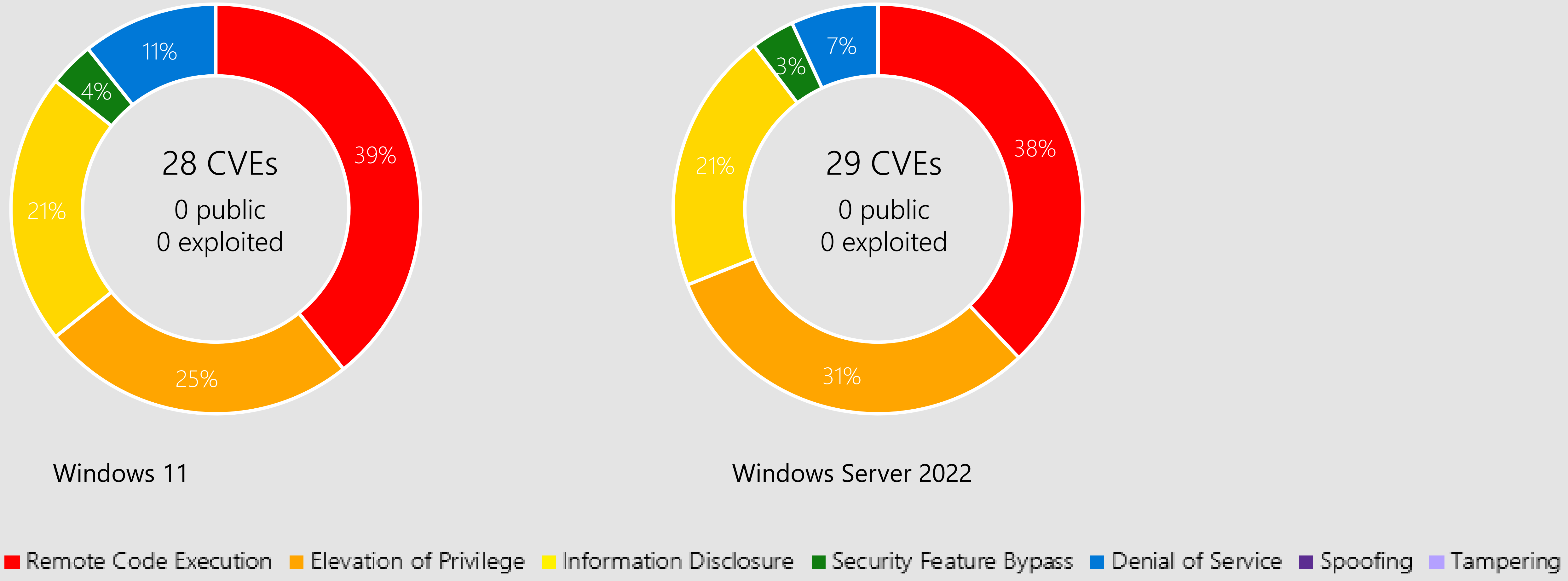
- Security Updates
- Security Advisory
- Product Support Lifecyle
- Other resources related to the release

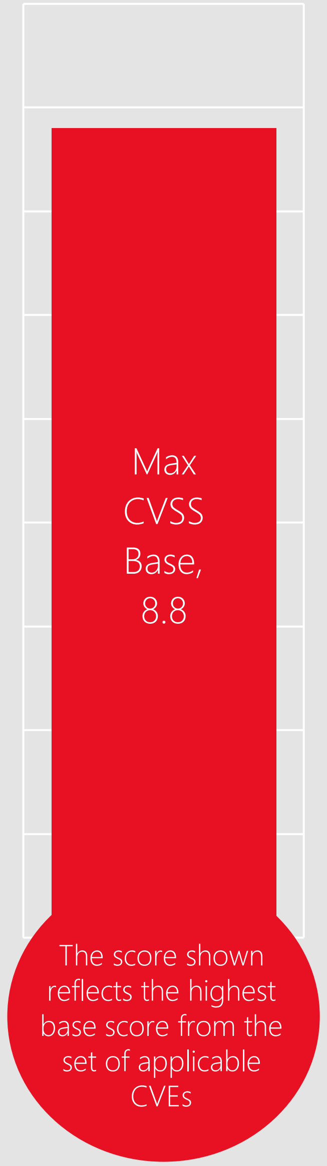
Monthly Security Release Overview - June 2022



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:

Advanced Local Procedure Call
AFD for WinSock
Container Isolation FS Filter Driver
Container Manager Service
EFS
File History
File Server Shadow Copy Agent Service (RVSS)
Hyper-V
Installer
iSCSI Discovery Service
Kerberos
LDAP
LSASS
Kerberos AppContainer
Kernel
Desired State Configuration (DSC)
Defender Remote Credential Guard

CVE-2022-30190 MSDT

Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly disclosed | Exploitation detected

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

Disable MSDT (Microsoft Support Diagnostic Tool) URL protocol handler. See MSRC blog for details

Affected Software

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

CVE-2022-30163 Hyper-V

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.

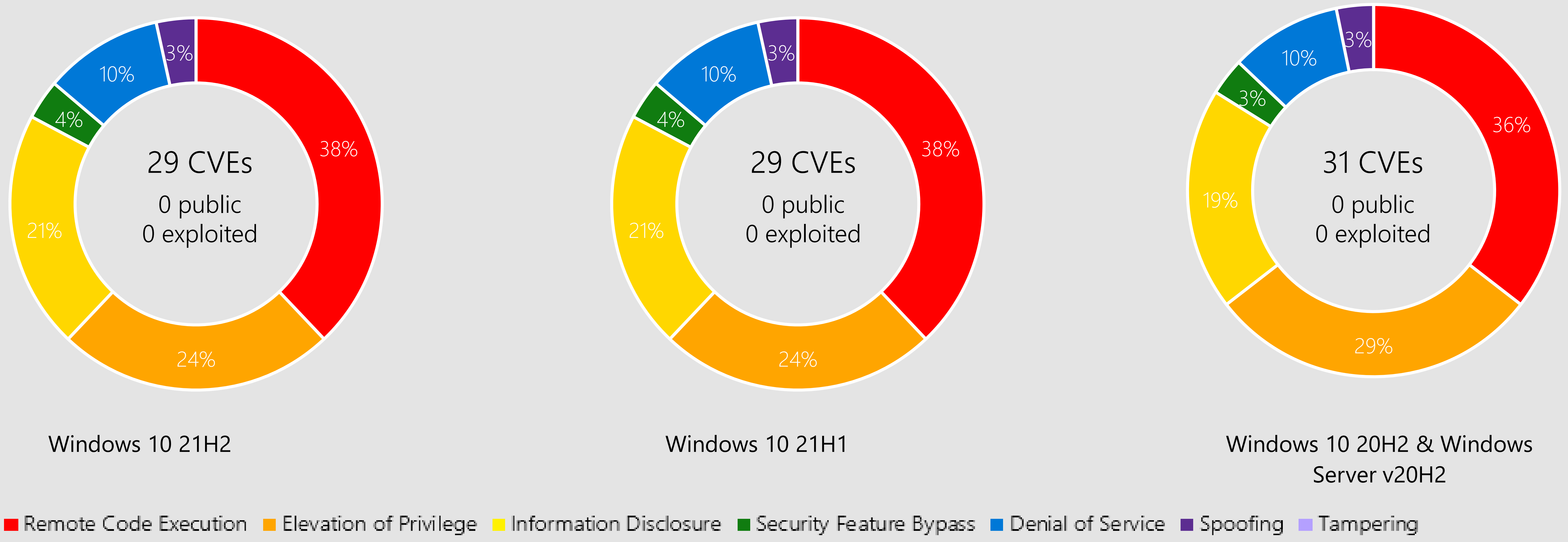
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

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

Windows 10



Windows 10 21H2

Windows 10 21H1

Windows 10 20H2 & Windows Server v20H2

Max CVSS Base, 9.8

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

Affected Components:

- Advanced Local Procedure Call
- AFD for WinSock
- Container Isolation FS Filter Driver
- Container Manager Service
- EFS
- File History
- File Server Shadow Copy Agent Service (RVSS)
- Hyper-V
- Installer
- iSCSI Discovery Service
- Kerberos
- LDAP
- LSASS
- Kerberos AppContainer
- NAT
- Desired State Configuration (DSC)
- NFS
- SMB
- Defender Remote Credential Guard
- Kernel

CVE-2022-30136 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 NFSV4.1
Warning: Do NOT apply this mitigation if May 2022 are not installed. See CVE entry for details.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2022-30165 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.

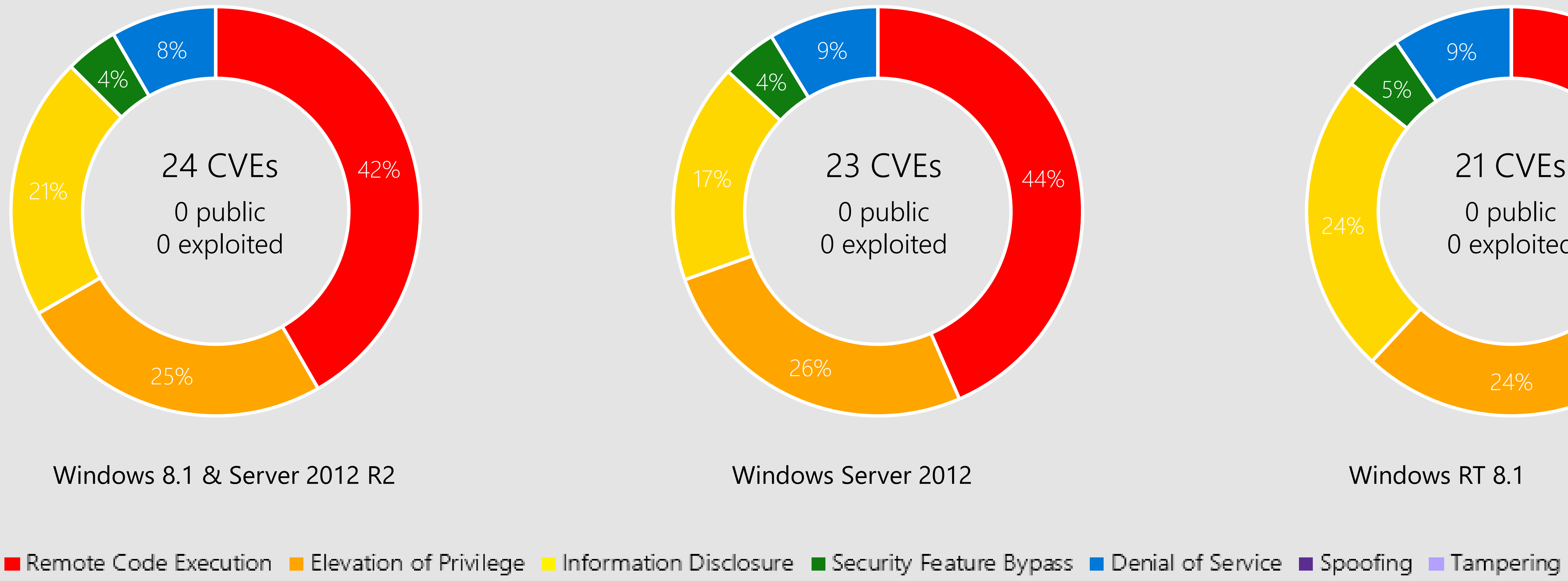
More Information

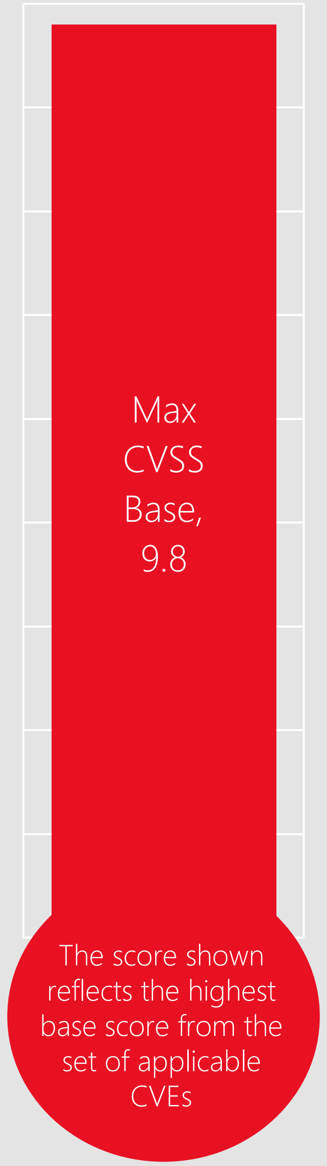
Systems configured to activate both of the following features in Windows Server: CredSSP (Credential Security Service Provider) and RCG (Remote Credential Guard) might be vulnerable to this exploit.

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





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

Affected Components:

- Advanced Local Procedure Call
- AFD for WinSock
- File History
- File Server Shadow Copy Agent Service (RVSS)
- Hyper-V
- Installer
- iSCSI Discovery Service
- Kerberos AppContainer
- Kernel
- LDAP
- LSASS
- Media Center
- NAT
- NFS

CVE-2022-30153 LDAP

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-2022-30164 Kerberos AppContainer

Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

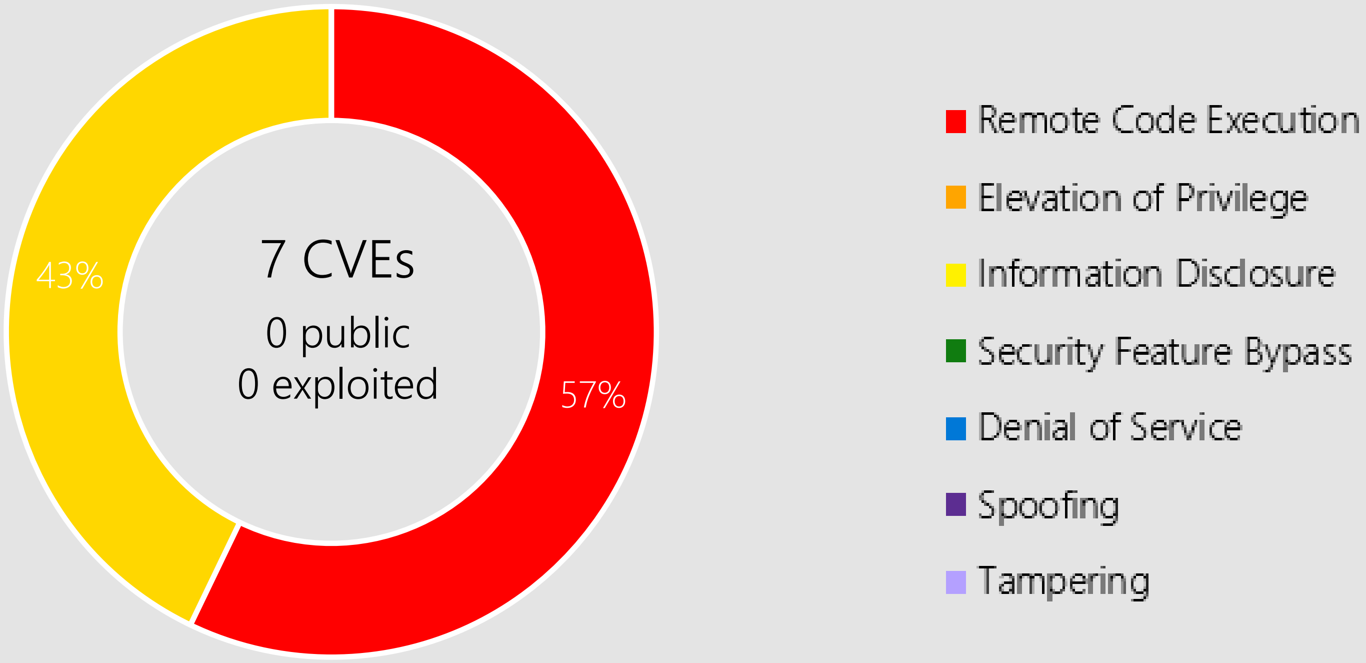
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
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:

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

CVE-2022-30157 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 2019
SharePoint Server Subscription Edition
SharePoint Enterprise Server 2016
SharePoint Enterprise Server 2013

CVE-2022-30173 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 Web Apps Server 2013
Excel 2013
Excel 2016

Other Products

SQL Server

CVE-2022-29143 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: SQL Server 2014, SQL Server 2016, SQL Server 2017, SQL Server 2019

Other Products

.NET 6.0, .NET Core

CVE-2022-30184 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET 6.0, .NET Core 3.1, NuGet.exe, Visual Studio 2019, Visual Studio 2022, Visual Studio 2019 for Mac, Visual Studio 2022 for Mac

Other Products

Visual Studio

CVE-2022-30184 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: .NET 6.0, .NET Core 3.1, NuGet.exe, Visual Studio 2019, Visual Studio 2022, Visual Studio 2019 for Mac, Visual Studio 2022 for Mac

Other Products

Azure Open Management Infrastructure (OMI)

CVE-2022-29149 | 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: Azure Automation State Configuration, DSC Extension, Azure Automation Update Management, Azure Diagnostics (LAD), Azure Open Management Infrastructure, Azure Security Center, Azure Sentinel, Azure Stack Hub, Container Monitoring Solution, Log Analytics Agent, System Center Operations Manager (SCOM) 2016, System Center Operations Manager (SCOM) 2019, System Center Operations Manager (SCOM) 2022

Note: Many services consume OMI. For a list of Microsoft services and recommended actions, please see CVE-2022-29149

Other Products

Azure Service Fabric Container

CVE-2022-30137 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.7
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Azure Service Fabric Linux clusters

What is being fixed in CVE-2022-30137?

Azure Service Fabric team is releasing a patch to further strengthen the security in the Linux cluster by adapting the principle of path to least privilege. Windows cluster are NOT impacted by this vulnerability.

Other Products

Azure RTOS GUIX

CVE-2022-30177/30178/30179 | 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: Azure Real Time Operating System GUIX.

CVE-2022-30180 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Azure Real Time Operating System GUIX

Security Advisory ADV220002

Overview

On June 14, 2022, Intel published information about a class of memory-mapped I/O vulnerabilities known as Processor MMIO Stale Data Vulnerabilities.

- CVE-2022-21123 - Shared Buffer Data Read (SBDR)
- CVE-2022-21125 - Shared Buffers Data Sampling (SBDS)
- CVE-2022-21127 - Special Register Buffer Data Sampling Update (SRBDS Update)
- CVE-2022-21166 - Device Register Partial Write (DRPW)

Microsoft has released software updates to help mitigate these vulnerabilities. To get all available protections, firmware (microcode) and software updates are required. Please check with your OEM for microcode updates. Microsoft has no information to indicate that these vulnerabilities have been used to attack customers at this time.

Suggested Actions:

Please see the ADV220002 for detail on recommend actions as well as potential performance impacts.

ADV220002 - Microsoft Guidance on Intel Processor MMIO Stale Data Vulnerabilities

Product Lifecycle Update

Fixed Policy End of Support

Internet Explorer 11*

Modern Policy Retirements

Dynamics 365 Field Service (on-prem)

aka.ms/lifecycle

Internet Explorer 11 desktop app retirement FAQ - Microsoft Tech Community

Known Issues

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

Customers who have the File Server VSS Agent Service running on their Windows Servers must install the June 14, 2022 or later Windows updates on both the Application Server and the File Server, to become protected and functional. Failure to install the updates on both machine roles could cause backup operations carried out by applications that previously worked to fail. For more information, see **https://support.microsoft.com/help/5015527**

Microsoft

Questions?

Appendix

CVE-2021-26414 Windows DCOM

KB5004442—Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)

- Hardening changes in DCOM were required for CVE-2021-26414. Therefore, we recommended that you verify if client or server applications in your environment that use DCOM or RPC work as expected with the hardening changes enabled.
  - The Distributed Component Object Model (DCOM) Remote Protocol is a protocol for exposing application objects using remote procedure calls (RPCs). DCOM is used for communication between the software components of networked devices.
- Microsoft is addressing this vulnerability in a phased rollout. The initial deployment phase starts with the Windows updates released on June 8, 2021. The updates will enable customers to verify that any client/server applications in their environment work as expected with the hardening changes enabled.
- Timeline

Update release	Behavior change
June 8, 2021	Hardening changes disabled by default but with the ability to enable them using a registry key.
June 14, 2022	Hardening changes enabled by default but with the ability to disable them using a registry key.
March 14, 2023	Hardening changes enabled by default with no ability to disable them. By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment.

CVE	Public	Exploited	Product
CVE-2022-29111	No	No	HEVC Video Extensions
CVE-2022-22018	No	No	HEVC Video Extensions
CVE-2022-30131	No	No	Container Isolation FS Filter Driver
CVE-2022-30132	No	No	Container Manager Service
CVE-2022-30135	No	No	Media Center
CVE-2022-30136	No	No	Network File System
CVE-2022-30140	No	No	iSCSI Discovery Service
CVE-2022-30141	No	No	Lightweight Directory Access Protocol (LDAP)
CVE-2022-30142	No	No	File History
CVE-2022-30143	No	No	LDAP
CVE-2022-30145	No	No	EFS
CVE-2022-30148	No	No	Desired State Configuration (DSC)
CVE-2022-30149	No	No	LDAP
CVE-2022-30150	No	No	Defender Remote Credential Guard

CVE	Public	Exploited	Product
CVE-2022-30151	No	No	Ancillary Function Driver for WinSock
CVE-2022-30152	No	No	Network Address Translation (NAT)
CVE-2022-30153	No	No	LDAP
CVE-2022-30155	No	No	Kernel
CVE-2022-30160	No	No	Advanced Local Procedure Call
CVE-2022-30161	No	No	LDAP
CVE-2022-30162	No	No	Kernel
CVE-2022-30163	No	No	Hyper-V
CVE-2022-30164	No	No	Kerberos AppContainer
CVE-2022-30167	No	No	AV1 Video Extension
CVE-2022-30188	No	No	HEVC Video Extensions
CVE-2022-29119	No	No	HEVC Video Extensions
CVE-2022-30139	No	No	LDAP
CVE-2022-30146	No	No	LDAP

CVE	Public	Exploited	Product
CVE-2022-30147	No	No	Installer
CVE-2022-30165	No	No	Kerberos
CVE-2022-30166	No	No	LSASS
CVE-2022-30168	No	No	Photos App
CVE-2022-30189	No	No	Autopilot Device Management and Enrollment Client
CVE-2022-30191	No	No	AV1 Video Extension
CVE-2022-32230	No	No	SMB
CVE-2022-30193	No	No	AV1 Video Extension
CVE-2022-30157	No	No	SharePoint Server
CVE-2022-30158	No	No	SharePoint Server
CVE-2022-30159	No	No	Office
CVE-2022-30171	No	No	Office
CVE-2022-30172	No	No	Office

CVE	Public	Exploited	Product
CVE-2022-30173	No	No	Excel
CVE-2022-30174	No	No	Office
CVE-2022-21166	No	No	Intel: CVE-2022-21166
CVE-2022-21127	No	No	Intel: CVE-2022-21127
CVE-2022-21123	No	No	Intel: CVE-2022-21123
CVE-2022-21125	No	No	Intel: CVE-2022-21125
CVE-2022-29149	No	No	Azure Open Management Infrastructure
ADV220002	No	No	Guidance on Intel Processor MMIO Stale Data Vulnerabilities
CVE-2022-30137	No	No	Azure Service Fabric Container
CVE-2022-30154	No	No	File Server Shadow Copy Agent Service (RVSS)
CVE-2022-30177	No	No	Azure RTOS GUIX Studio
CVE-2022-30178	No	No	Azure RTOS GUIX Studio
CVE-2022-30179	No	No	Azure RTOS GUIX Studio
CVE-2022-30180	No	No	Azure RTOS GUIX Studio

CVE	Public	Exploited	Product
CVE-2022-30184	No	No	.NET and Visual Studio
CVE-2022-29143	No	No	SQL Server