Microsoft

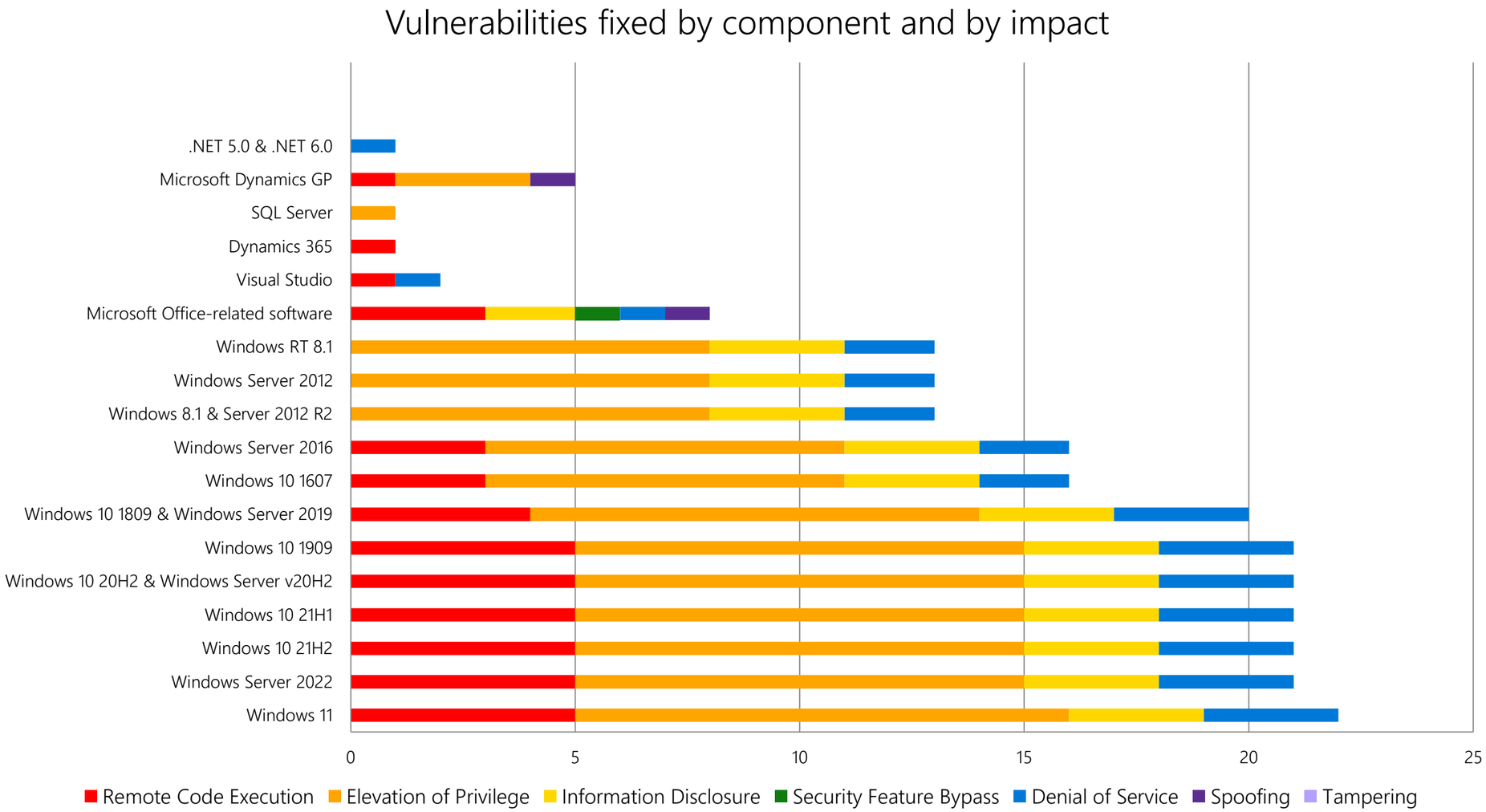
Microsoft Security Release

February 8, 2022

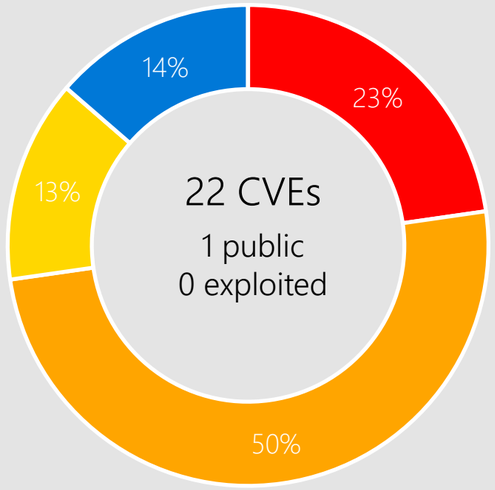
Agenda

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

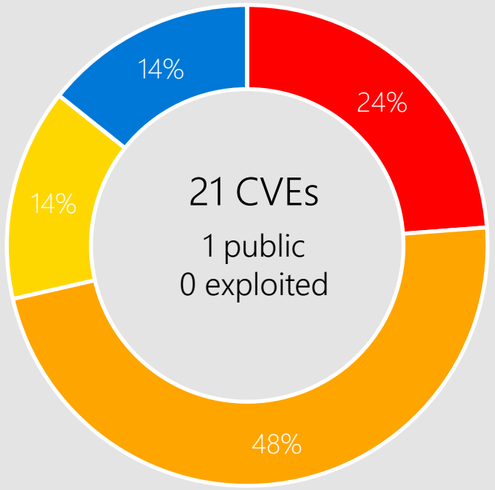
Monthly Security Release Overview - February 2022



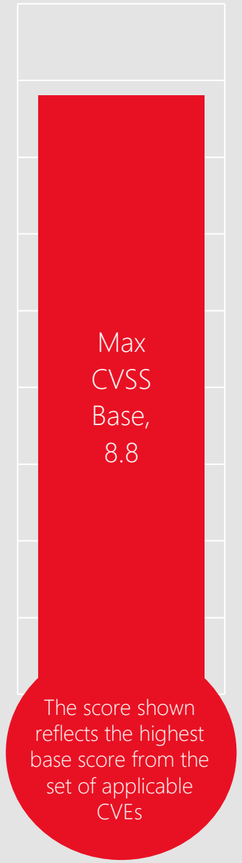
Windows 11, Server 2022



Windows 11



Windows Server 2022



Remote Code Execution | Elevation of Privilege | Information Disclosure | Security Feature Bypass | Denial of Service | Spoofing | Tampering

Affected Components:

Common Log File System Driver
DNS Server
DWM Core Library
Hyper-V
Kernel
Mobile Device Management
Named Pipe File System
Print Spooler
Remote Access Connection Manager
Roaming Security Rights Management Services
Runtime
Services for NFS ONCRPC XDR Driver

CVE-2022-21984 DNS 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

To be vulnerable, a DNS server would need to have dynamic updates enabled.

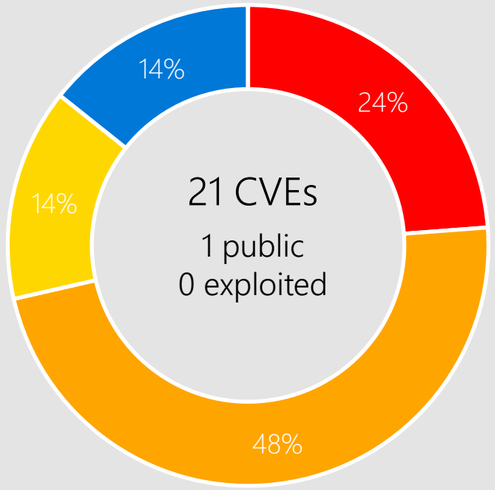
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

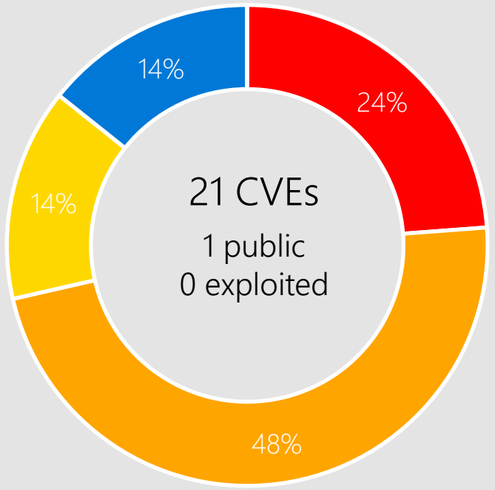
Affected Software

Windows 11
Server 2022
Server, version 20H2
Windows 10

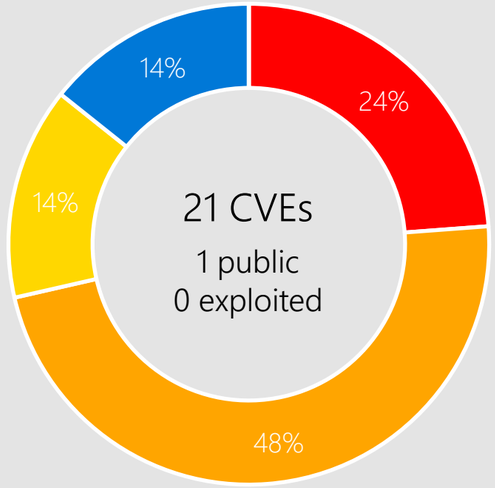
Windows 10



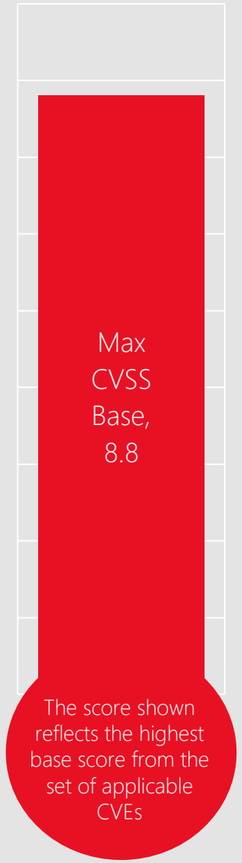
Windows 10 21H2



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

Affected Components:

Common Log File System Driver
DNS Server
DWM Core Library
Hyper-V
Kernel
Mobile Device Management
Named Pipe File System
Print Spooler
Remote Access Connection Manager
Roaming Security Rights Management Services
Runtime
Services for NFS ONCRPC XDR Driver

CVE-2022-21989 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.

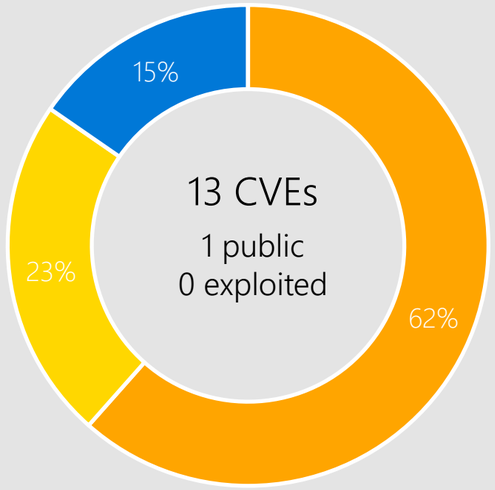
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

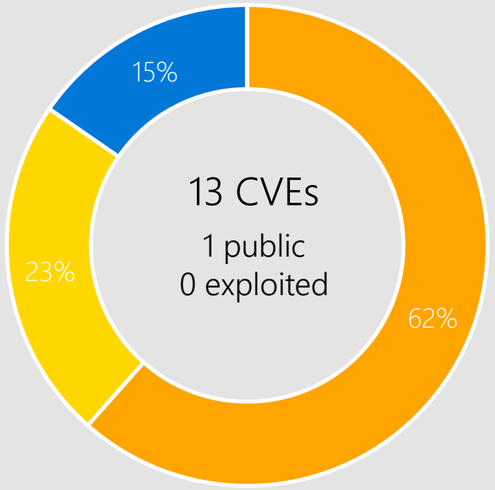
Affected Software

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

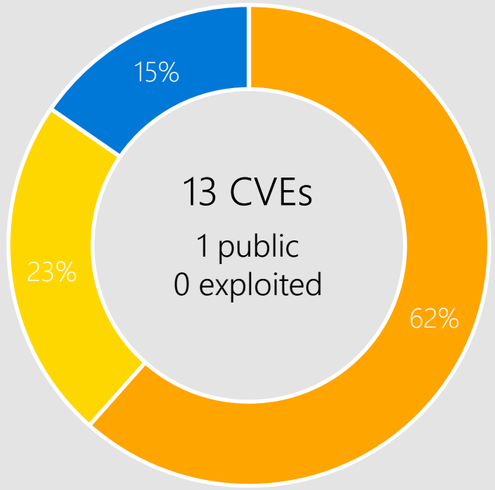
Windows 8.1, Server 2012 R2, and Server 2012



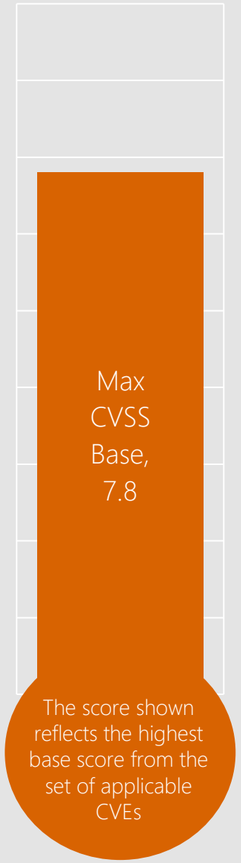
Windows 8.1 & Server 2012 R2



Windows Server 2012



Windows RT 8.1



Remote Code Execution Elevation of Privilege Information Disclosure Security Feature Bypass Denial of Service Spoofing Tampering

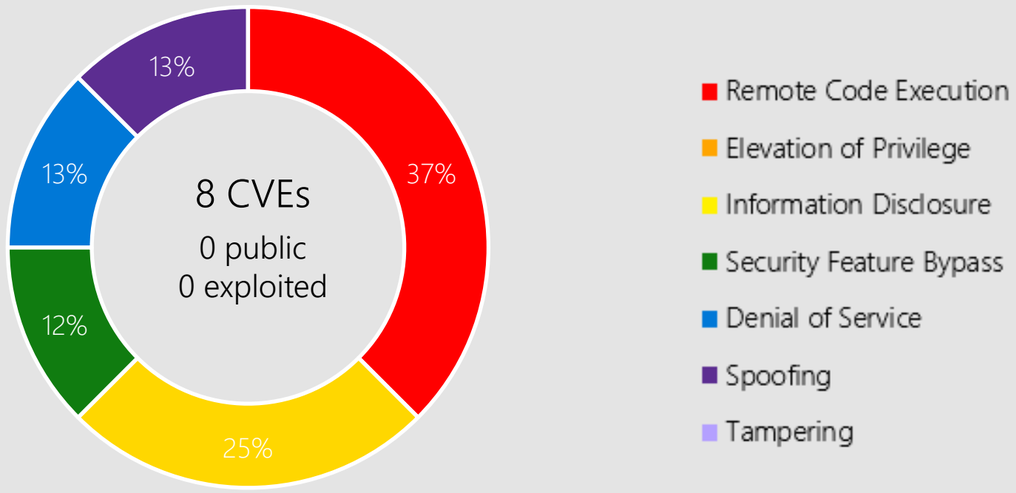
Affected Components:

Common Log File
System Driver
Kernel
Print Spooler

Remote Access
Connection Manager
Services for NFS

ONCRPC XDR Driver
User Account Profile
Picture

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2013 Click-to-Run (C2R)/2016/2019
Outlook 2016 for Mac
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
OneDrive Android
SharePoint Foundation 2013
SharePoint Server Subscription Edition
Teams Android
Teams iOS
Teams Admin Center

CVE-2022-22005 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-2022-22003 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
Office 2016
Office 2013
Office LTSC for Mac 2021
Office 2019
Office 2019 for Mac
365 Apps Enterprise

Other Products

SQL Server

CVE-2022-23276 | 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: SQL Server 2019 Linux Containers.

Other Products

Dynamics 365

CVE-2022-21957 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 8.2.

Other Products

Microsoft Dynamics GP

CVE-2022-23274 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics GP.

Other Products

Microsoft Dynamics GP

CVE-2022-23272 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics GP.

CVE-2022-23273 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics GP.

Other Products

Microsoft Dynamics GP

CVE-2022-23269 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.9
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: Required
Products: Dynamics GP.

CVE-2022-23271 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics GP.

Other Products

.NET 5.0 and .NET 6.0

CVE-2022-21986 | 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: Visual Studio 2022 version 17.0, Visual Studio 2019 for Mac version 8.10, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), .NET 5.0, .NET 6.0.

Other Products

Visual Studio

CVE-2022-21986 | 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: Visual Studio 2022 version 17.0, Visual Studio 2019 for Mac version 8.10, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), .NET 5.0, .NET 6.0.

CVE-2022-21991 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.1
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Visual Studio Code.

Other Products

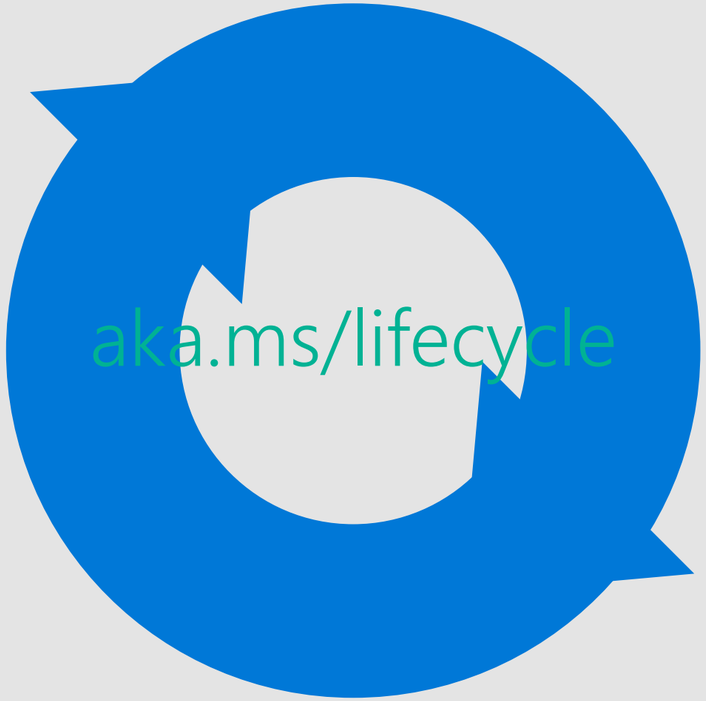
Azure Data Explorer, Power BI

CVE-2022-23256 Azure Data Explorer
CVE-2022-23254 Power BI Desktop

Product Lifecycle Update

Products reaching end of support in February

Dynamics 365 for Talent



Helping customers shift to a modern desktop

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-21971	No	No	Runtime
CVE-2022-21981	No	No	Common Log File System Driver
CVE-2022-21844	No	No	HEVC Video Extensions
CVE-2022-21926	No	No	HEVC Video Extensions
CVE-2022-21927	No	No	HEVC Video Extensions
CVE-2022-22709	No	No	VP9 Video Extensions
CVE-2022-22710	No	No	Common Log File System Driver
CVE-2022-22712	No	No	Hyper-V
CVE-2022-22715	No	No	Named Pipe File System
CVE-2022-22717	No	No	Print Spooler
CVE-2022-22718	No	No	Print Spooler
CVE-2022-21984	No	No	DNS Server
CVE-2022-21985	No	No	Remote Access Connection Manager
CVE-2022-21989	Yes	No	Kernel

CVE	Public	Exploited	Product
CVE-2022-21992	No	No	Mobile Device Management
CVE-2022-21993	No	No	Services for NFS ONCRPC XDR Driver
CVE-2022-21994	No	No	DWM Core Library
CVE-2022-21995	No	No	Hyper-V
CVE-2022-21996	No	No	Win32k
CVE-2022-21997	No	No	Print Spooler
CVE-2022-21998	No	No	Common Log File System Driver
CVE-2022-21999	No	No	Print Spooler
CVE-2022-22000	No	No	Common Log File System Driver
CVE-2022-22001	No	No	Remote Access Connection Manager
CVE-2022-22002	No	No	User Account Profile Picture
CVE-2022-22003	No	No	Office Graphics

CVE	Public	Exploited	Product
CVE-2022-23263	No	No	Edge (Chromium-based)
CVE-2022-21987	No	No	SharePoint Server
CVE-2022-21988	No	No	Office Visio
CVE-2022-21968	No	No	SharePoint Server
CVE-2022-22716	No	No	Excel
CVE-2022-22004	No	No	Office ClickToRun
CVE-2022-22005	No	No	SharePoint Server
CVE-2022-23252	No	No	Office
CVE-2022-23280	No	No	Outlook for Mac
CVE-2022-21974	No	No	Roaming Security Rights Management Services
CVE-2022-21957	No	No	Dynamics 365 (on-premises)
CVE-2022-21965	No	No	Teams
CVE-2022-23254	No	No	Power BI
CVE-2022-23269	No	No	Dynamics GP

CVE	Public	Exploited	Product
CVE-2022-23271	No	No	Dynamics GP Elevation Of Privilege
CVE-2022-23272	No	No	Dynamics GP Elevation Of Privilege
CVE-2022-23273	No	No	Dynamics GP Elevation Of Privilege
CVE-2022-23274	No	No	Dynamics GP
CVE-2022-23276	No	No	SQL Server for Linux Containers
CVE-2022-21986	No	No	Kestrel Web Server
CVE-2022-21991	No	No	Visual Studio Code Remote Development Extension
CVE-2022-23255	No	No	OneDrive for Android
CVE-2022-23256	No	No	Azure Data Explorer