Microsoft

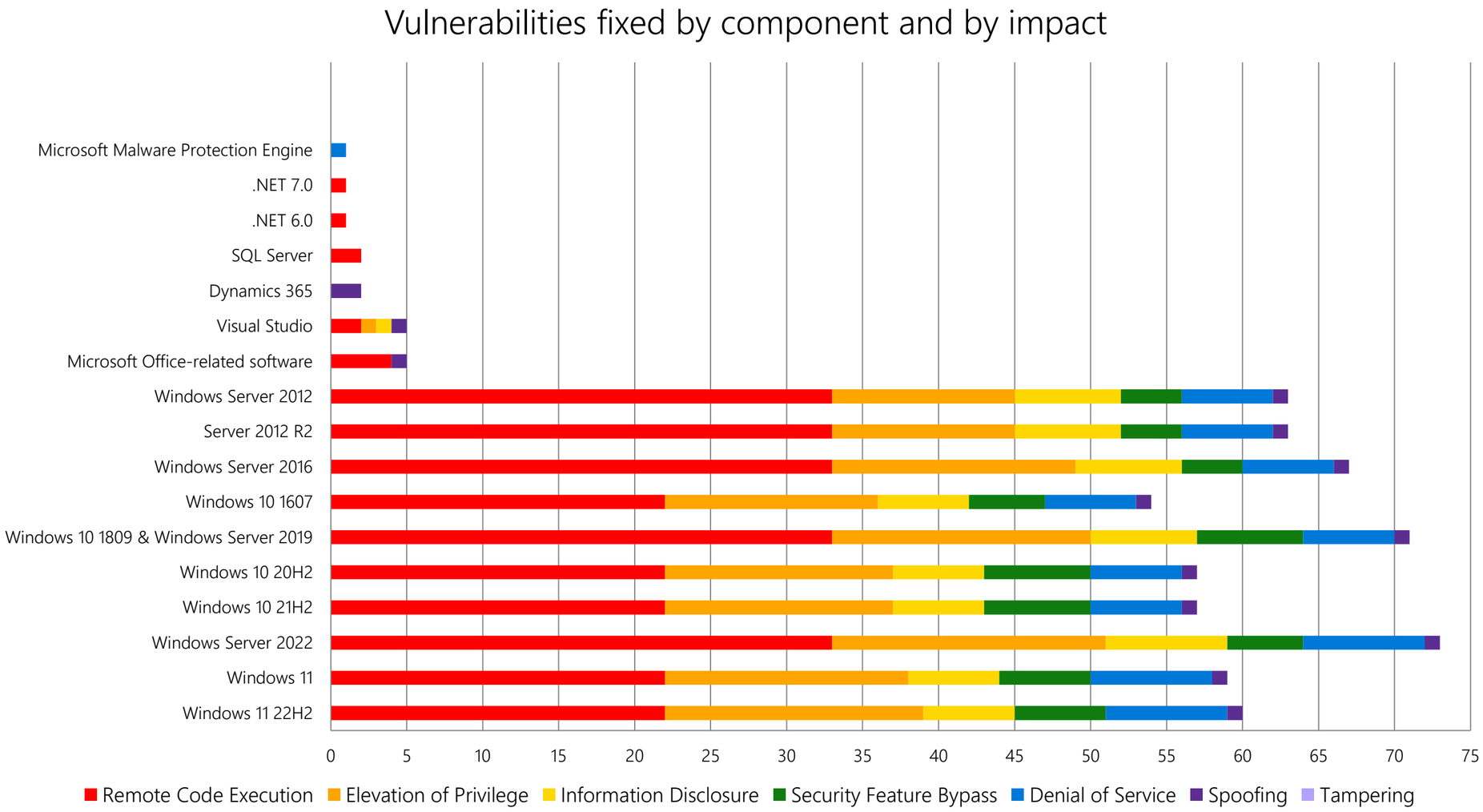
Microsoft Security Release

April 11, 2023

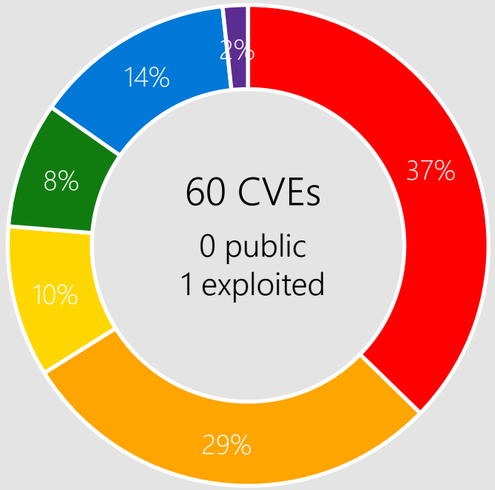
Agenda

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

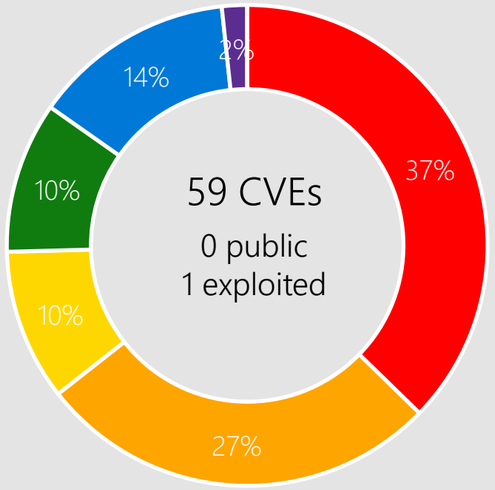
Monthly Security Release Overview - April 2023



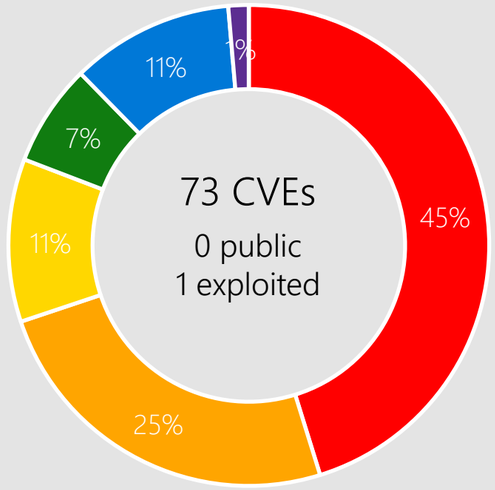
Windows 11, Server 2022



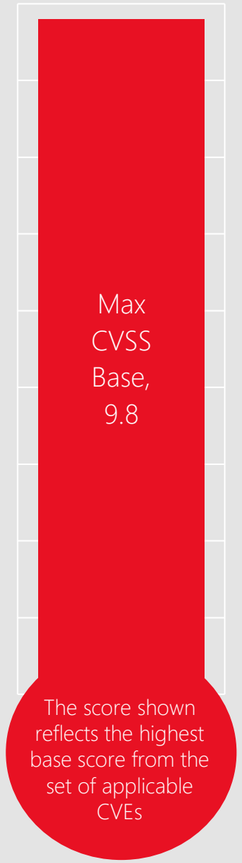
Windows 11 22H2



Windows 11



Windows Server 2022



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

Affected Components:

See appendix for details

CVE-2023-21554 Message Queuing

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 message queuing service needs to be enabled for a system to be exploitable.
Check for Message Queuing service and TCP 1801 listening

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-28250 PGM

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 message queuing service needs to be enabled for a system to be exploitable.
Check for Message Queuing service and TCP 1801 listening

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-21727 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.

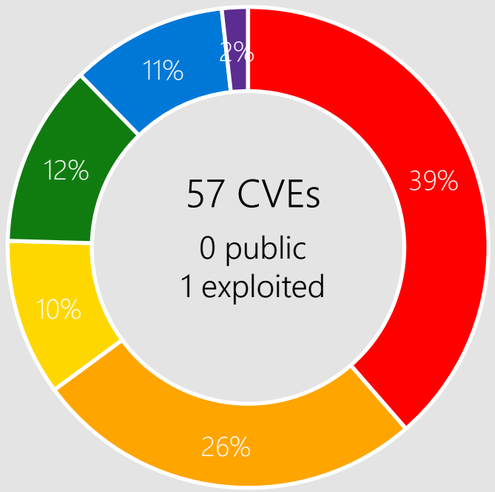
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

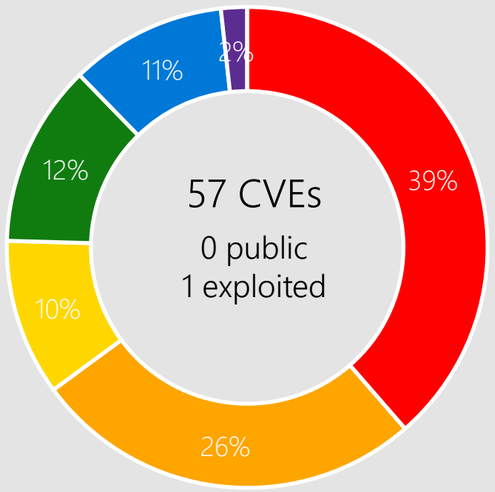
Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

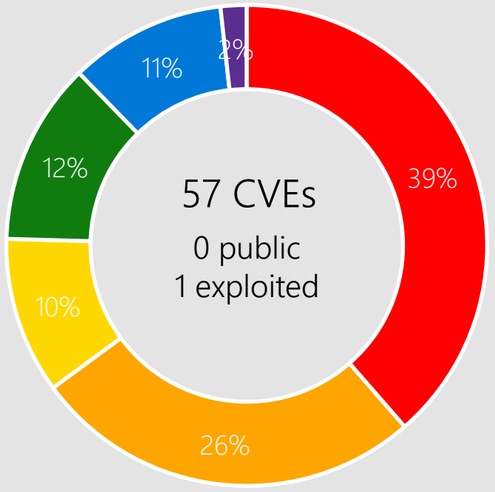
Windows 10



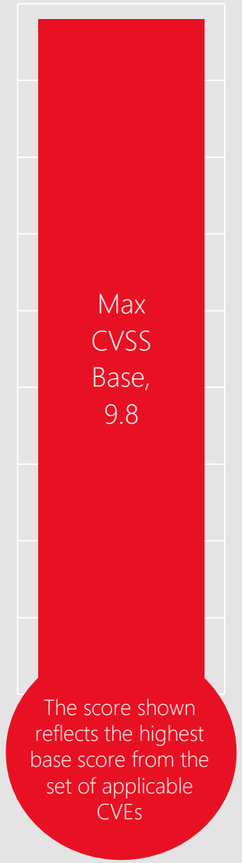
Windows 10 22H2



Windows 10 21H2



Windows 10 20H2



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

Affected Components:

See appendix for details

CVE-2023-28252 Common Log File System Driver

Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

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.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-28231 DHCP Server Service

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Adjacent | 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

Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-28219 Layer 2 Tunneling Protocol

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.

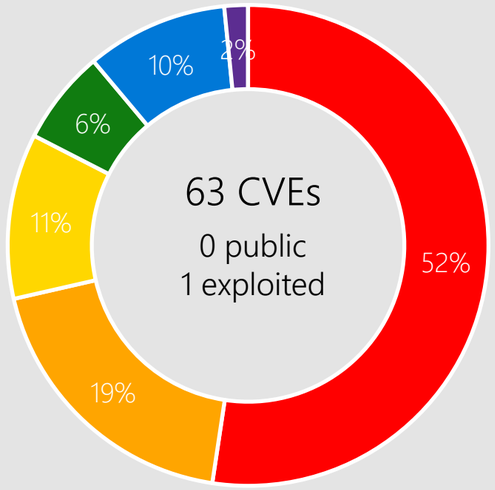
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

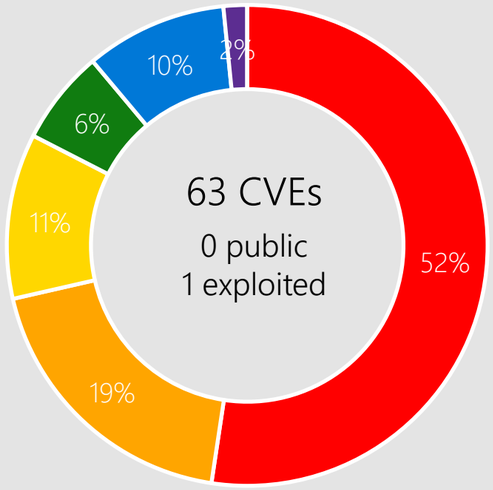
Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

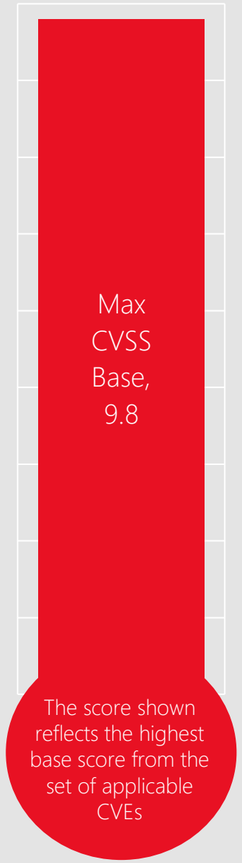
Windows Server 2012 R2, and Server 2012



Server 2012 R2



Windows Server 2012



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

Affected Components:

See appendix for details

CVE-2023-28240 Network Load Balancing

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Adjacent | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Migrate from **Network Load Balancing** to **Software Load Balancing**.
Microsoft recommends that customer using Network Load Balancing migrate their deployments to the newer Software Load Balancing solution

Affected Software

Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2023-24884 Printer Drivers

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 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

CVE-2023-28275 WDAC OLE DB Provider

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.

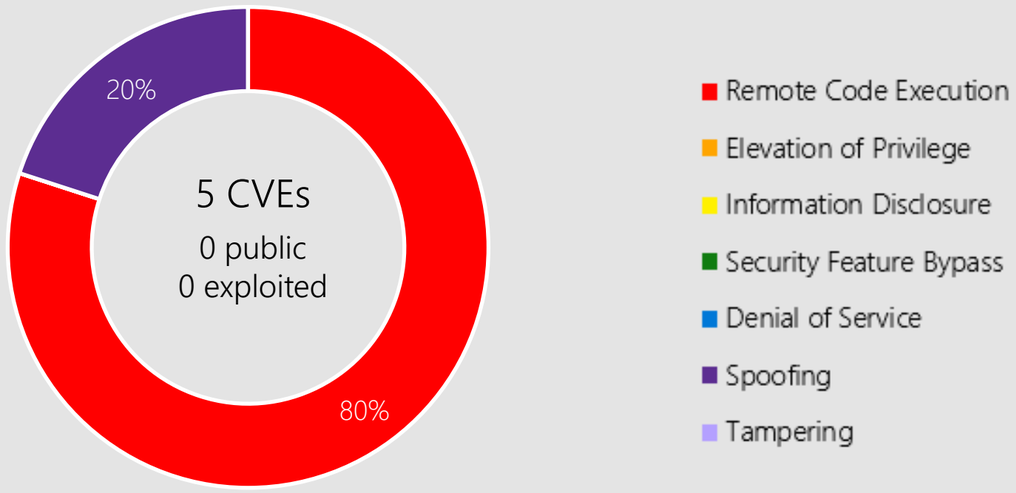
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

- Windows 11 22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012

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
Publisher 2013
Publisher 2016
SharePoint Foundation 2013
SharePoint Server Subscription Edition

CVE-2023-28285 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 for Mac 2021
365 Apps Enterprise
Office 2019 for Mac

CVE-2023-28287 Publisher

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 2019
Office LTSC 2021
Publisher 2016
Publisher 2013

CVE-2023-28288 SharePoint Server

Impact, Severity, Disclosure

Spoofing | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 6.5 | 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

Other Products

Dynamics 365

CVE-2023-28309 | 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 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0, Dynamics 365 Field Service (on-premises) v7 series.

CVE-2023-28313 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Send Customer Voice survey from Dynamics 365.

Other Products

Dynamics 365

CVE-2023-28314 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

Other Products

SQL Server ODBC Driver

CVE-2023-23375 | 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: Microsoft ODBC Driver 17 for SQL Server, Microsoft ODBC Driver 18 for SQL Server, Microsoft OLE DB Driver 18 for SQL Server, Microsoft OLE DB Driver 19 for SQL Server

CVE-2023-28304 | 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: Microsoft ODBC Driver 17 for SQL Server, Microsoft ODBC Driver 18 for SQL Server, Microsoft OLE DB Driver 18 for SQL Server, Microsoft OLE DB Driver 19 for SQL Server

Other Products

.NET 6.0 and .NET 7.0

CVE-2023-28260 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: .NET 6.0, .NET 7.0.

Other Products

Microsoft Malware Protection Engine

CVE-2023-24860 | 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: Malware Protection Engine.

Other Products

Visual Studio

CVE-2023-28296 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.4
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-28260 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.5, .NET 6.0, .NET 7.0.

Other Products

Visual Studio

CVE-2023-24893 | 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 Code.

CVE-2023-28262 | 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: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Visual Studio

CVE-2023-28263 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

CVE-2023-28299 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2022 version 17.0, Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.5, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10).

Other Products

Azure

CVE-2023-28300 Azure Service Connector

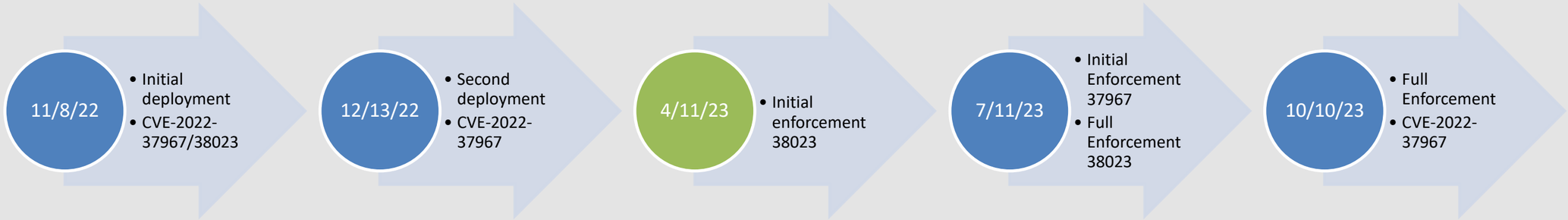
CVE-2023-28312 Azure for Machine Learning

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.



Suggested Actions:

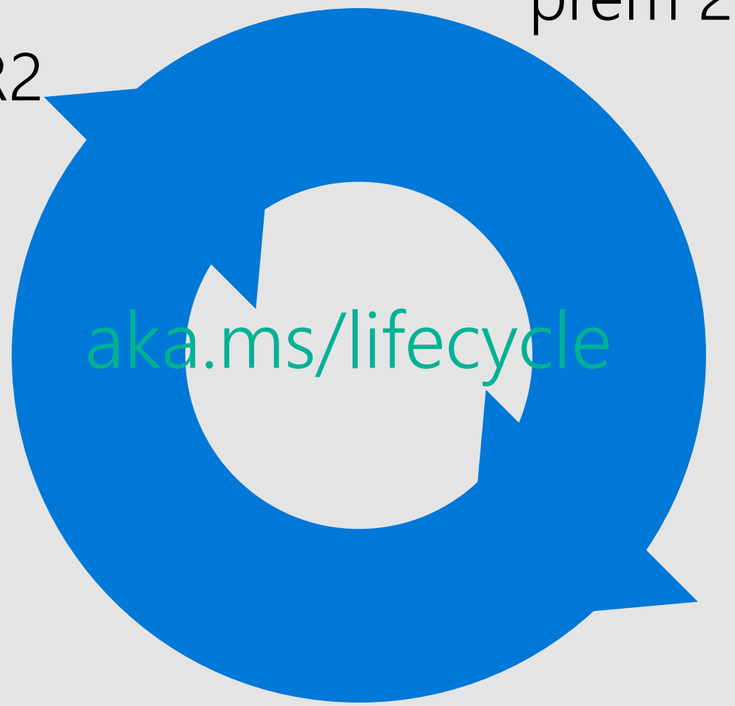
1. Review CVE entries including the FAQ section to understand risks
2. Review the Knowledge Base articles for details on deployment and enforcement of these changes

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

Product Lifecycle Update

Products retiring in April

Exchange 2013
Office 2013
Dynamics GP 2013 and 2013 R2
Lync 2013



Modern Policy

Dynamics 365 Business Central on-prem 2021 release wave 2, version 19.x

[Latest Servicing Stack Updates]

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2023-21727	No	No	Remote Procedure Call Runtime
CVE-2023-21729	No	No	Remote Procedure Call Runtime
CVE-2023-24914	No	No	Win32k
CVE-2023-24931	No	No	Secure Channel
CVE-2023-28216	No	No	ALPC
CVE-2023-28217	No	No	Network Address Translation (NAT)
CVE-2023-28218	No	No	Ancillary Function Driver for WinSock
CVE-2023-28221	No	No	Error Reporting Service
CVE-2023-28222	No	No	Kernel
CVE-2023-28285	No	No	Office Graphics
CVE-2023-28291	No	No	Raw Image Extension
CVE-2023-28292	No	No	Raw Image Extension
CVE-2023-28297	No	No	RPCSS
CVE-2023-28298	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2023-28305	No	No	DNS Server
CVE-2023-24912	No	No	Graphics Component
CVE-2023-28219	No	No	Layer 2 Tunneling Protocol
CVE-2023-28220	No	No	Layer 2 Tunneling Protocol
CVE-2023-28223	No	No	Domain Name Service
CVE-2023-28224	No	No	Point-to-Point Protocol over Ethernet (PPPoE)
CVE-2023-28225	No	No	NTLM
CVE-2023-28226	No	No	Enroll Engine
CVE-2023-28227	No	No	Bluetooth Driver
CVE-2023-28228	No	No	Windows
CVE-2023-28229	No	No	CNG Key Isolation Service
CVE-2023-28231	No	No	DHCP Server Service
CVE-2023-28232	No	No	Point-to-Point Tunneling Protocol
CVE-2023-28233	No	No	Secure Channel

CVE	Public	Exploited	Product
CVE-2023-28234	No	No	Secure Channel
CVE-2023-28235	No	No	Lock Screen
CVE-2023-28236	No	No	Kernel
CVE-2023-28237	No	No	Kernel
CVE-2023-28238	No	No	IKE Protocol Extensions
CVE-2023-28240	No	No	Network Load Balancing
CVE-2023-28241	No	No	SSTP
CVE-2023-28266	No	No	CLFS Driver
CVE-2023-28267	No	No	Remote Desktop Protocol Client
CVE-2023-28244	No	No	Kerberos
CVE-2023-28268	No	No	Netlogon RPC
CVE-2023-28246	No	No	Registry
CVE-2023-28270	No	No	Lock Screen
CVE-2023-28247	No	No	Network File System

CVE	Public	Exploited	Product
CVE-2023-28248	No	No	Kernel
CVE-2023-28271	No	No	Kernel Memory
CVE-2023-28272	No	No	Kernel
CVE-2023-28250	No	No	Pragmatic General Multicast (PGM)
CVE-2023-28273	No	No	Clip Service
CVE-2023-28274	No	No	Win32k
CVE-2023-28252	No	Yes	Common Log File System Driver
CVE-2023-28253	No	No	Kernel
CVE-2023-28276	No	No	Group Policy
CVE-2023-28254	No	No	DNS Server
CVE-2023-28277	No	No	DNS Server
CVE-2023-28255	No	No	DNS Server
CVE-2023-28278	No	No	DNS Server

CVE	Public	Exploited	Product
CVE-2023-28256	No	No	DNS Server
CVE-2023-28293	No	No	Kernel
CVE-2023-28302	No	No	Message Queuing
CVE-2023-28306	No	No	DNS Server
CVE-2023-28307	No	No	DNS Server
CVE-2023-28308	No	No	DNS Server
CVE-2023-28284	No	No	Edge (Chromium-based)
CVE-2023-24935	No	No	Edge (Chromium-based)
CVE-2023-28301	No	No	Edge (Chromium-based)
CVE-2023-28287	No	No	Publisher
CVE-2023-28288	No	No	SharePoint Server
CVE-2023-28295	No	No	Publisher
CVE-2023-28311	No	No	Word
CVE-2023-21769	No	No	Message Queuing

CVE	Public	Exploited	Product
CVE-2023-23384	No	No	SQL Server
CVE-2023-28300	No	No	Azure Service Connector
CVE-2023-28309	No	No	D365 (on-premises)
CVE-2023-28313	No	No	D365 Customer Voice
CVE-2023-28314	No	No	D365 (on-premises)
CVE-2023-24893	No	No	Visual Studio Code
CVE-2023-21554	No	No	Message Queuing
CVE-2023-23375	No	No	SQL Server
CVE-2023-24860	No	No	Defender
CVE-2023-24924	No	No	PS & PCL6 Printer Driver
CVE-2023-24883	No	No	PS & PCL6 Printer Driver
CVE-2023-24925	No	No	PS & PCL6 Printer Driver
CVE-2023-24884	No	No	PS & PCL6 Printer Driver
CVE-2023-24926	No	No	PS & PCL6 Printer Driver

CVE	Public	Exploited	Product
CVE-2023-24885	No	No	PS & PCL6 Printer Driver
CVE-2023-24927	No	No	PS & PCL6 Printer Driver
CVE-2023-24886	No	No	PS & PCL6 Printer Driver
CVE-2023-24928	No	No	PS & PCL6 Printer Driver
CVE-2023-24887	No	No	PS & PCL6 Printer Driver
CVE-2023-24929	No	No	PS & PCL6 Printer Driver
CVE-2023-28243	No	No	PS & PCL6 Printer Driver
CVE-2023-28275	No	No	WDAC OLE DB provider for SQL Server
CVE-2023-28260	No	No	.NET DLL Hijacking
CVE-2023-28262	No	No	Visual Studio
CVE-2023-28263	No	No	Visual Studio
CVE-2023-28296	No	No	Visual Studio
CVE-2023-28299	No	No	Visual Studio
CVE-2023-28304	No	No	SQL Server

CVE	Public	Exploited	Product
CVE-2023-28312	No	No	Azure Machine Learning
CVE-2023-28249	No	No	Boot Manager
CVE-2023-28269	No	No	Boot Manager