Microsoft

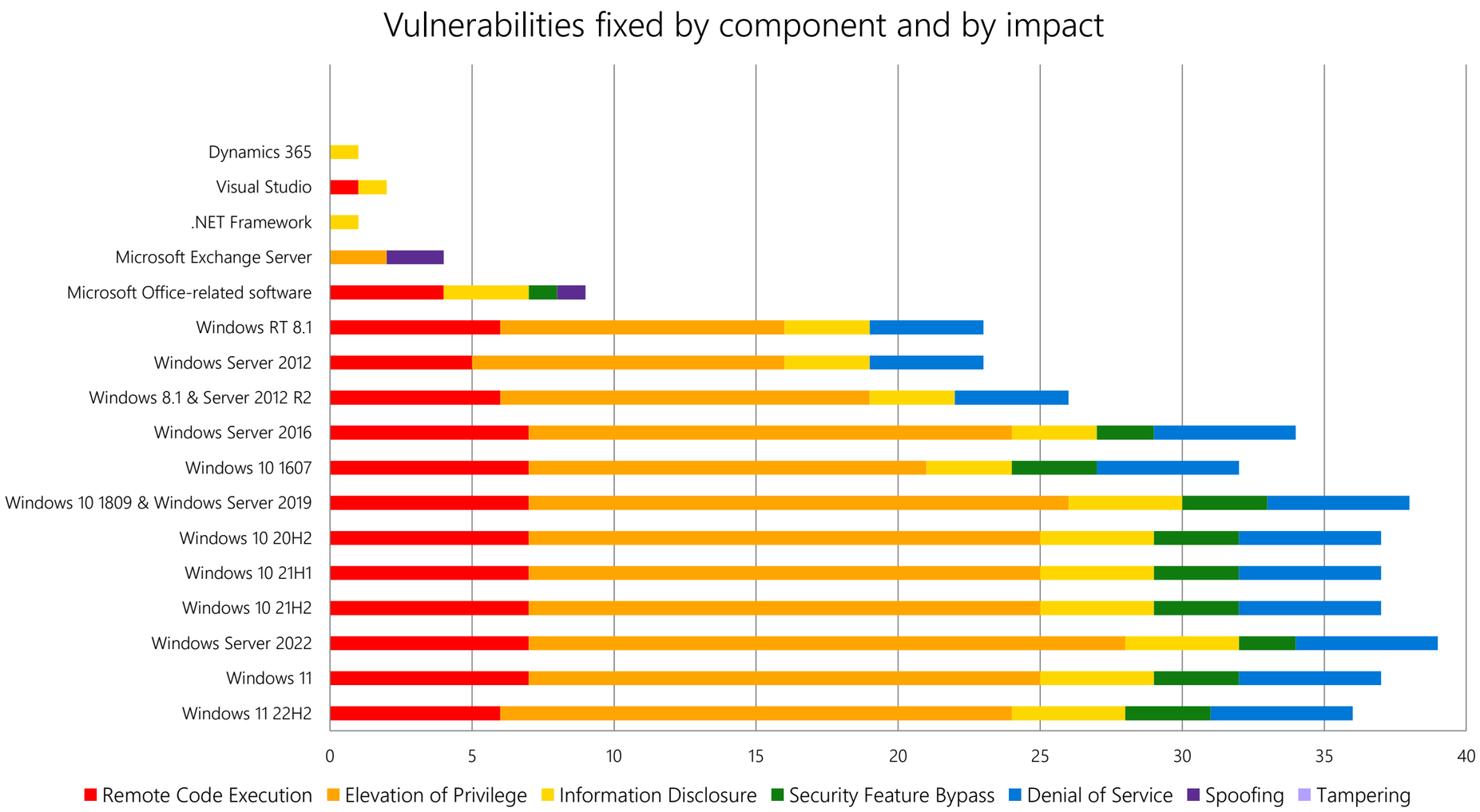
Microsoft Security Release

November 8, 2022

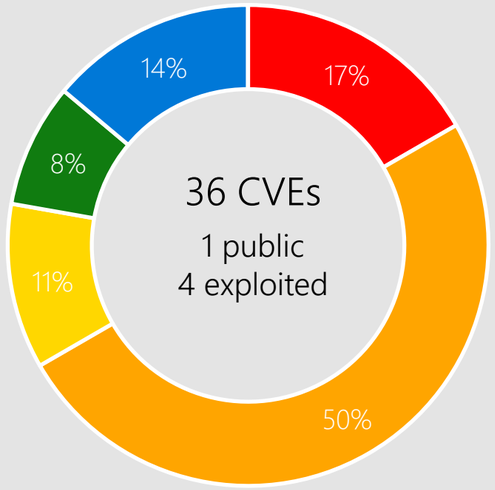
Agenda

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

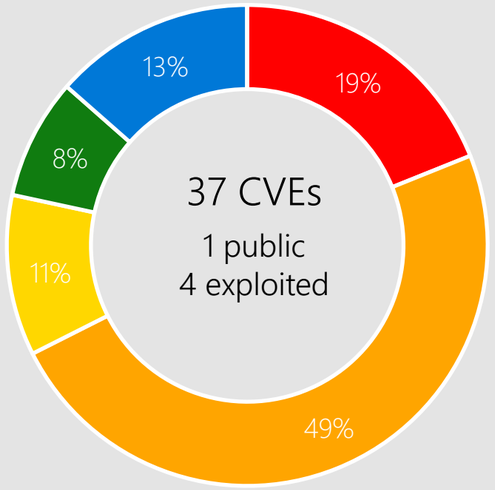
Monthly Security Release Overview - November 2022



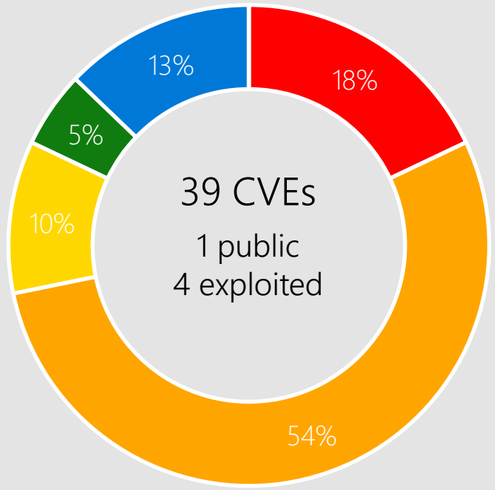
Windows 11, Server 2022



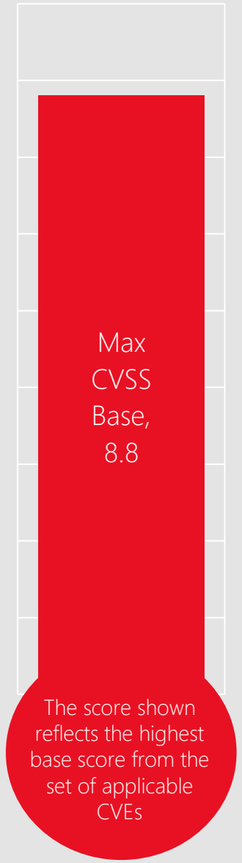
Windows 11 22H2



Windows 11



Windows Server 2022



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

Affected Components:

Please see Appendix for complete list.

CVE-2022-41128 Scripting Languages

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | Exploitation detected

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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Windows 8.1

CVE-2022-41125 CNG Key Isolation Service

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.

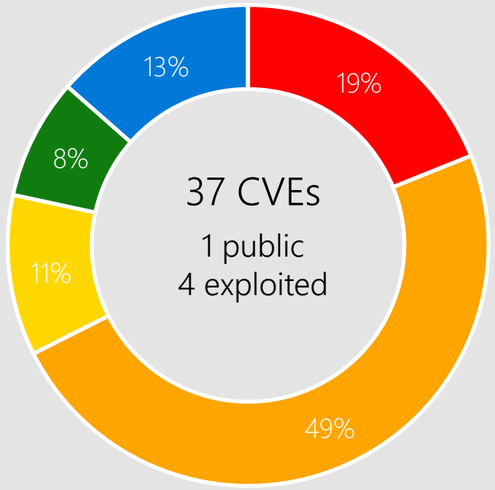
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

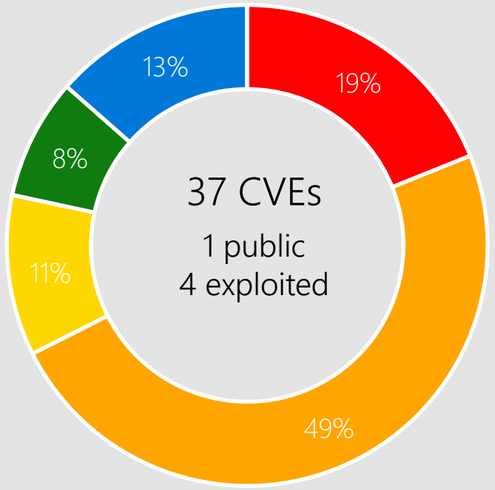
Affected Software

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

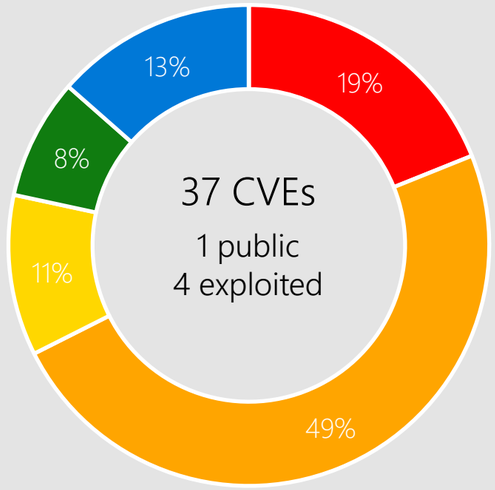
Windows 10



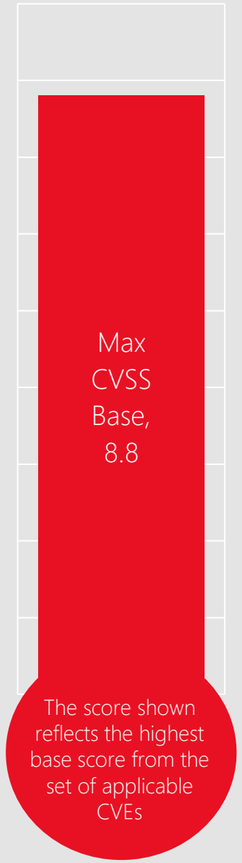
Windows 10 22H2



Windows 10 21H2



Windows 10 21H1



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

Affected Components:

Please see Appendix for complete list.

CVE-2022-41073 Print Spooler

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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

CVE-2022-41047 ODBC Driver

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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

CVE-2022-41091 MOTW

Impact, Severity, Disclosure

Security Feature Bypass | Important | Publicly disclosed | Exploitation Detected

CVSSScoreMetrics

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

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

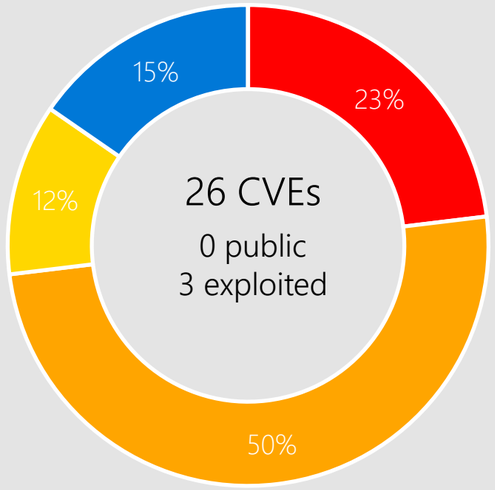
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

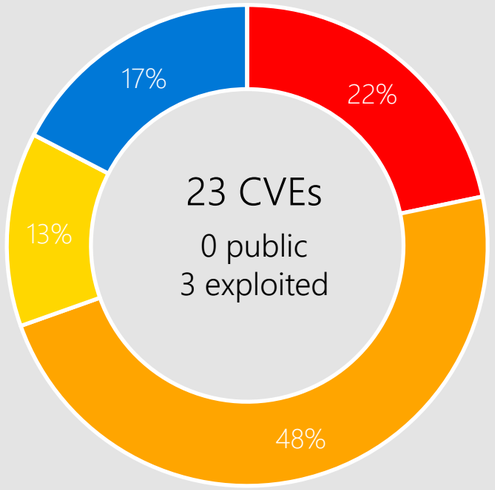
Affected Software

Windows 11 22H2
Windows 11
Server 2022
Server 2019
Windows 10
Server 2016

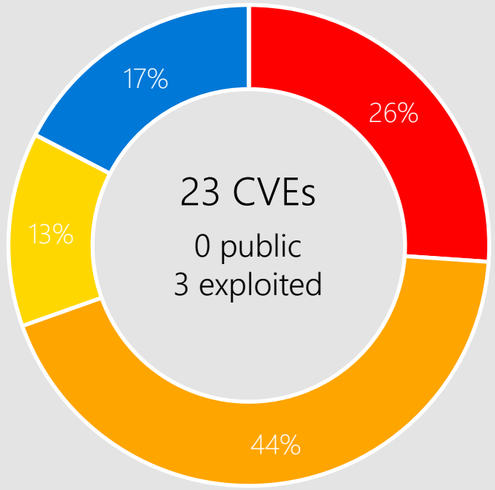
Windows 8.1, Server 2012 R2, and Server 2012



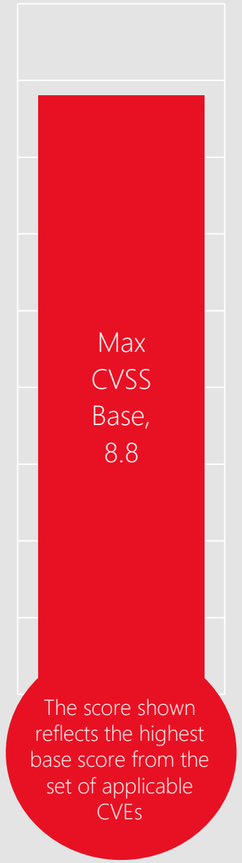
Windows 8.1 & Server 2012 R2



Windows Server 2012



Windows RT 8.1



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

Affected Components:

Advanced Local Procedure Call (ALPC)
CNG Key Isolation Service
Digital Media Receiver
GDI+
Group Policy
HTTP.sys
Kerberos
Kerberos RC4-HMAC
Netlogon RPC
Network Address Translation (NAT)
Network Policy Server (NPS) RADIUS Protocol
ODBC Driver
PPTP
Print Spooler

CVE-2022-41039 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

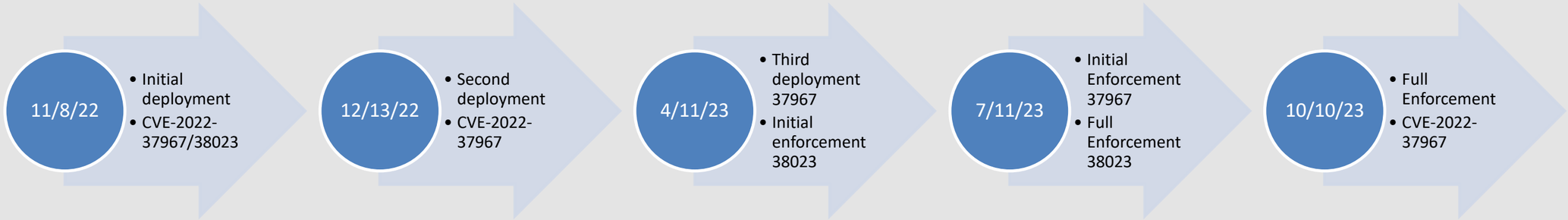
- Windows 11 22H2
- Windows 11
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

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.

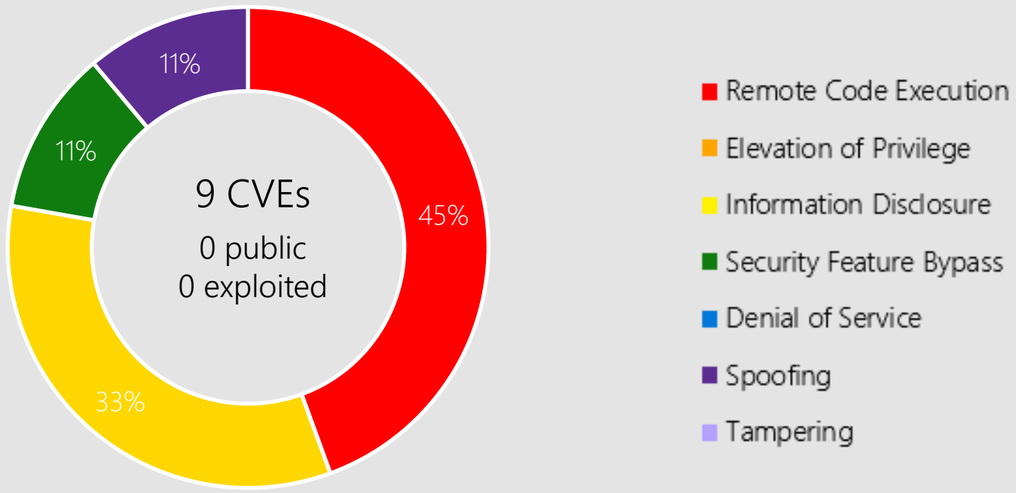


Suggested Actions:

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

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Word 2013/2016
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
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Server Subscription Edition Language Pack

CVE-2022-41062 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 Server 2019
- SharePoint Enterprise Server 2016
- SharePoint Enterprise Server 2013

CVE-2022-41107 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
Office LTSC 2021
365 Apps Enterprise
Office 2019
Office 2019 for Mac

CVE-2022-41063 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

Excel 2016
Excel 2013
Office Web Apps Server 2013
Office LTSC 2021
Office 2019
Office Online Server
365 Apps Enterprise

Other Products

Exchange Server

CVE-2022-41082 (previously released 9/30/2022) | Critical | Remote Code Execution | Public: No | Exploited: Yes

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

CVE-2022-41040 (previously released 9/30/2022) | Critical | Elevation of Privilege | Public: No | Exploited: Yes

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

Other Products

Exchange Server

CVE-2022-41080 | Critical | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

CVE-2022-41123 | 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: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

Other Products

Exchange Server

CVE-2022-41078 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22.

CVE-2022-41079 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

Other Products

Dynamics Business Central

CVE-2022-41066 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 4.4
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
User Interaction: None
Products: Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.5

Other Products

.NET Framework

CVE-2022-41064 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.8
Attack Vector: Adjacent
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Nuget 4.8.5, Nuget 2.1.2, .NET Framework 4.8.1 on Windows 10 21H2, .NET Framework 4.6 on Server 2008, .NET Framework 4.8.1 on Windows 11 22H2, .NET Framework 4.8.1 on Windows 10 21H1, .NET Framework 4.8 on Windows 8.1, .NET Framework 4.7.2 on Windows 10 1809, .NET Framework 4.7.2 on Server 2019, .NET Framework 4.8.1 on Windows 10 1809, .NET Framework 4.8.1 on Windows 10 20H2, .NET Framework 4.8 on Windows 11 22H2, .NET Framework 4.8.1 on Windows 10 22H2, .NET Framework 4.8.1 on Windows 11, .NET Framework 4.8 on Windows 10 22H2, .NET Framework 4.8 on Windows 11, .NET Framework 4.8 on Server 2019, .NET Framework 4.8 on Windows 10 21H1, .NET Framework 4.8 on Windows 8.1 x64-based systems, .NET Framework 4.8 on Server 2008 R2, .NET Framework 4.8 on Windows 10 21H2, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.8 on Windows 10 1809, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Windows 7, .NET Framework 4.6/4.6.1/4.6.2 on Windows 10, .NET Framework 4.8 on Windows 10 1607, .NET Framework 4.8 on Windows 8.1 32-bit systems, .NET Framework 4.8 on Server 2016, .NET Framework 4.8 on Windows 10 20H2.

Other Products

Visual Studio

CVE-2022-41119 | 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 17.3, 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 2017 version 15.9 (includes 15.0 - 15.8).

CVE-2022-39253 | Important | Information Disclosure | Public: No | Exploited: No

The vulnerability assigned to this CVE is in Git for Windows software which is consumed by Microsoft Visual Studio. It is being documented in the Security Update Guide to announce that the latest builds of Visual Studio are no longer vulnerable.

Products: Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.3.

Other Products

Open SSL

CVE-2022-3602

CVSS Base Score : see OpenSSL Blog
More Information: Awareness and guidance related to OpenSSL 3.0-3.06 risk
Products: vcpkg, Azure Kubernetes Service, Azure SDK C++.

CVE-2022-3786

CVSS Base Score : see OpenSSL Blog
More Information: Awareness and guidance related to OpenSSL 3.0-3.06 risk
Products: vcpkg, Azure Kubernetes Service, Azure SDK C++.

Other Products

Azure and Windows Utilities

CVE-2022-39327 Azure CLI
CVE-2022-41085 Azure CycleCloud 8, Azure CycleCloud 7
CVE-2022-41051 AzureOS GUIX Studio
CVE-2022-41120 Windows Sysmon

Security Advisory ADV220003

Summary

Microsoft has released an update for Microsoft Office that provides enhanced security as a defense in depth measure. This update provides hardening around IRM-protected documents to ensure the trust-of-certificate chain.

Suggested Actions:

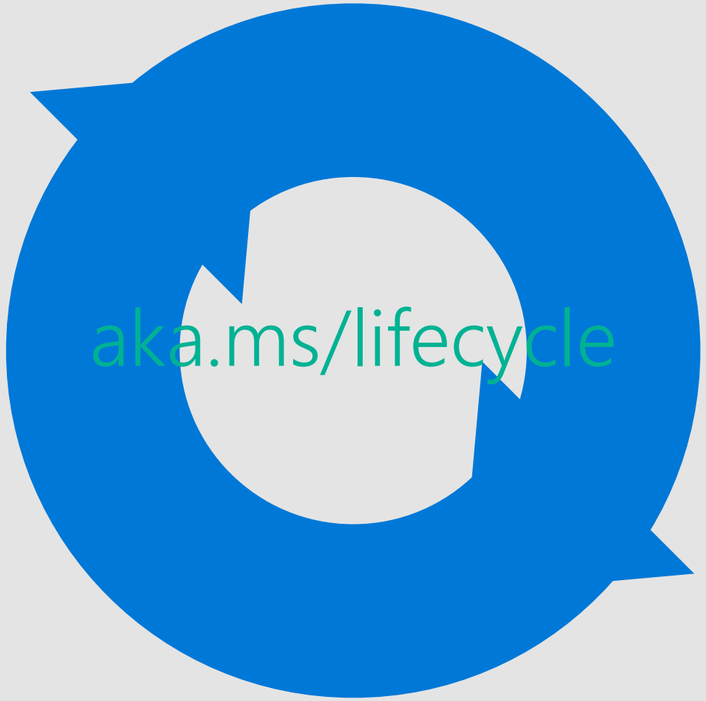
1. Apply the November Office updates

[ADV220003 - Security Update Guide - Microsoft - Microsoft Defense in Depth Update]

Product Lifecycle Update

Nothing reaching end of support in November

Windows 10 Semi-Annual Channel end of service
Windows 10 21H1 in December



ADV990001 - Security Update Guide - Microsoft - Latest Servicing Stack Updates

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2022-38014	No	No	Subsystem for Linux (WSL2) Kernel
CVE-2022-37966	No	No	Kerberos RC4-HMAC
CVE-2022-41100	No	No	Advanced Local Procedure Call (ALPC)
CVE-2022-41058	No	No	Network Address Translation (NAT)
CVE-2022-41101	No	No	Overlay Filter
CVE-2022-41102	No	No	Overlay Filter
CVE-2022-41120	No	No	Sysmon
CVE-2022-41128	No	Yes	Scripting Languages
CVE-2022-38015	No	No	Hyper-V
CVE-2022-37967	No	No	Kerberos
CVE-2022-38023	No	No	Netlogon RPC
CVE-2022-37992	No	No	Group Policy
CVE-2022-41039	No	No	Point-to-Point Tunneling Protocol
CVE-2022-41086	No	No	Group Policy

CVE	Public	Exploited	Product
CVE-2022-41044	No	No	Point-to-Point Tunneling Protocol
CVE-2022-41088	No	No	Point-to-Point Tunneling Protocol
CVE-2022-41045	No	No	Advanced Local Procedure Call (ALPC)
CVE-2022-41090	No	No	Point-to-Point Tunneling Protocol
CVE-2022-41047	No	No	ODBC Driver
CVE-2022-41048	No	No	ODBC Driver
CVE-2022-41091	Yes	Yes	Mark of the Web
CVE-2022-41092	No	No	Win32k
CVE-2022-41049	No	No	Mark of the Web
CVE-2022-41093	No	No	Advanced Local Procedure Call (ALPC)
CVE-2022-41050	No	No	Extensible File Allocation Table
CVE-2022-41052	No	No	Graphics Component
CVE-2022-41095	No	No	Digital Media Receiver
CVE-2022-41053	No	No	Kerberos

CVE	Public	Exploited	Product
CVE-2022-41096	No	No	DWM Core Library
CVE-2022-41054	No	No	Resilient File System (ReFS)
CVE-2022-41055	No	No	Human Interface Device
CVE-2022-41098	No	No	GDI+
CVE-2022-41099	No	No	BitLocker
CVE-2022-41057	No	No	HTTP.sys
CVE-2022-41107	No	No	Office Graphics
CVE-2022-41109	No	No	Win32k
CVE-2022-41113	No	No	Win32 Kernel Subsystem
CVE-2022-41114	No	No	Bind Filter Driver
CVE-2022-41116	No	No	Point-to-Point Tunneling Protocol
CVE-2022-41073	No	Yes	Print Spooler
CVE-2022-41118	No	No	Scripting Languages
CVE-2022-41125	No	Yes	CNG Key Isolation Service

CVE	Public	Exploited	Product
CVE-2022-41122	No	No	SharePoint Server
ADV220003	No	No	Office Defense in Depth Update
CVE-2022-41060	No	No	Word
CVE-2022-41103	No	No	Word
CVE-2022-41061	No	No	Word
CVE-2022-41104	No	No	Excel
CVE-2022-41105	No	No	Excel
CVE-2022-41062	No	No	SharePoint Server
CVE-2022-41106	No	No	Excel
CVE-2022-41063	No	No	Excel
CVE-2022-23824	No	No	AMD: CVE-2022-23824
CVE-2022-41085	No	No	Azure CycleCloud
CVE-2022-41064	No	No	.NET Framework
CVE-2022-39327	No	No	GitHub: CVE-2022-39327

CVE	Public	Exploited	Product
CVE-2022-41078	No	No	Exchange Server
CVE-2022-41123	No	No	Exchange Server
CVE-2022-41079	No	No	Exchange Server
CVE-2022-41080	No	No	Exchange Server
CVE-2022-3602	No	No	OpenSSL: CVE-2022-3602 X.509 certificate verification buffer overrun
CVE-2022-39253	No	No	GitHub: CVE-2022-39253
CVE-2022-41051	No	No	Azure RTOS GUIX Studio
CVE-2022-41097	No	No	Network Policy Server (NPS) RADIUS Protocol
CVE-2022-41056	No	No	Network Policy Server (NPS) RADIUS Protocol
CVE-2022-41066	No	No	Business Central
CVE-2022-41119	No	No	Visual Studio
CVE-2022-3786	No	No	OpenSSL: CVE-2022-3786