Microsoft

Microsoft Security Release

January 9, 2024

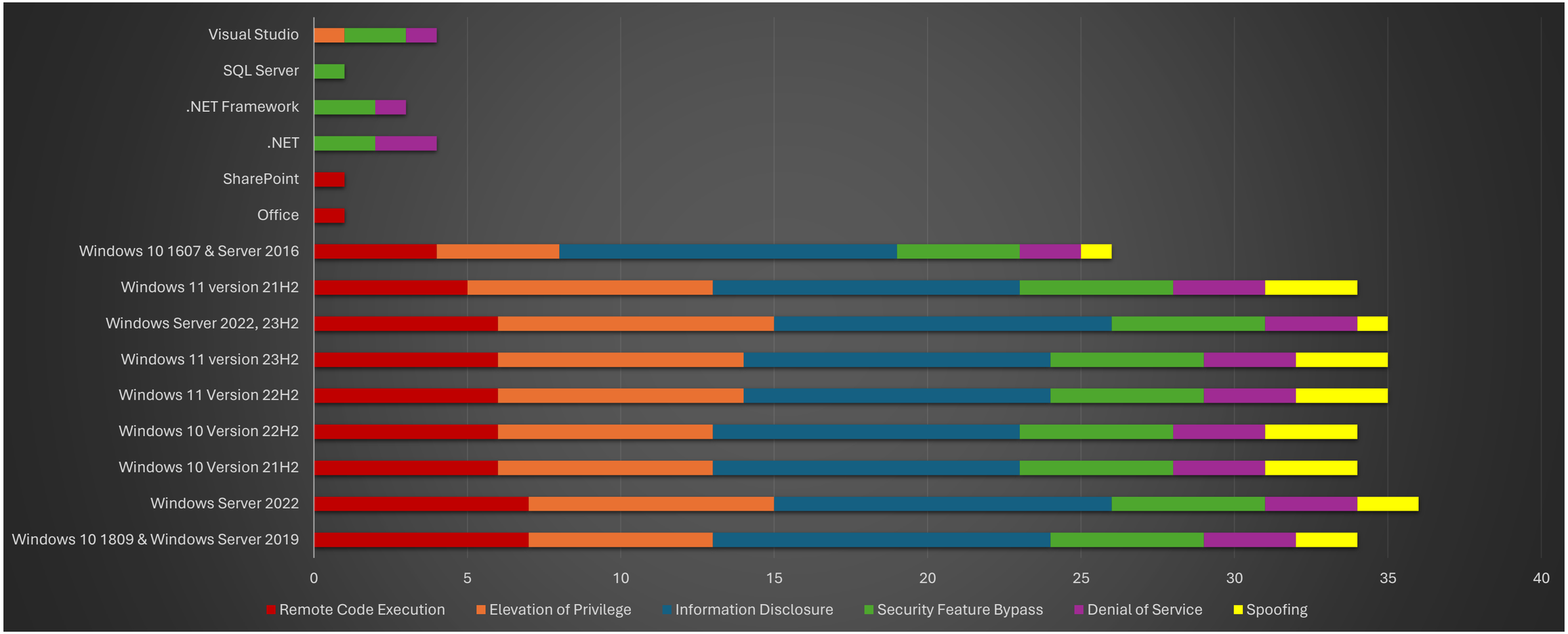
Agenda

Security Updates

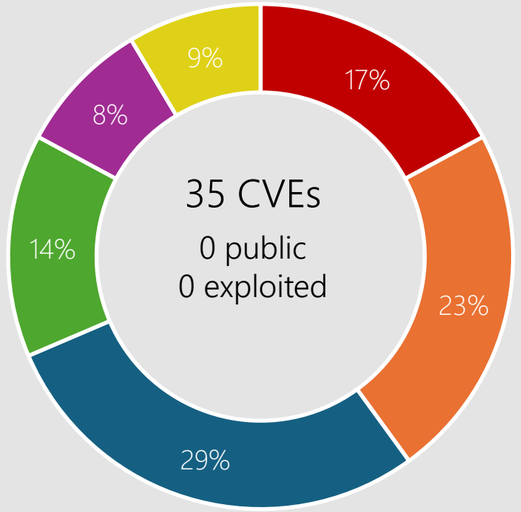
Security Advisory

Product Support Lifecyle

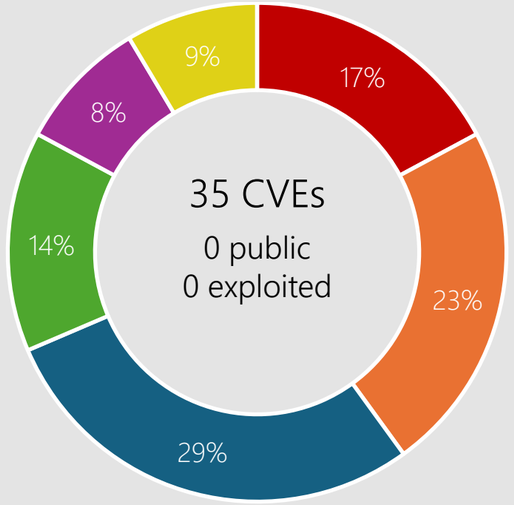
Microsoft Security Release Overview – January 2024



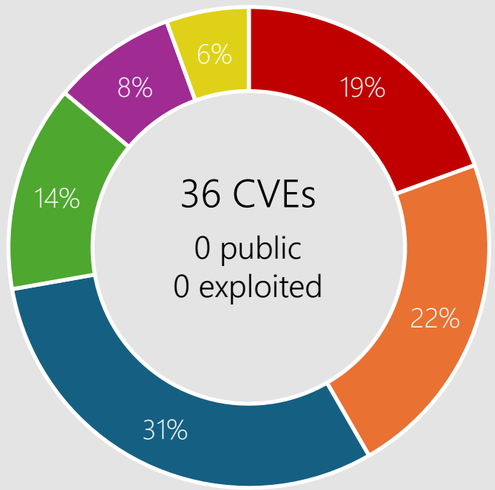
Windows 11, Server 2022



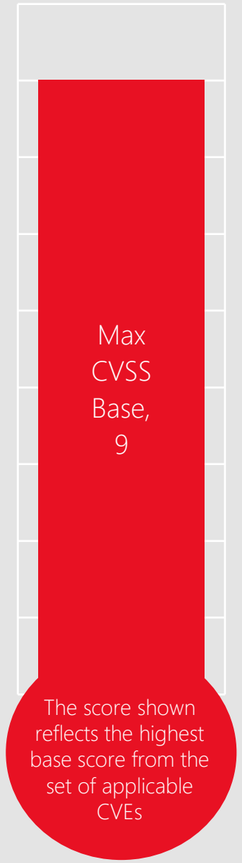
Windows 11 23H2



Windows 11 22H2



Windows Server 2022



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

Affected Components:

See appendix

CVE-2024-20674 Kerberos

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.0 | Attack Vector: Adjacent | 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
Windows 10
Server 2022
Server 2019
Server 2016

CVE-2024-20700 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Adjacent | Attack Complexity: High | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

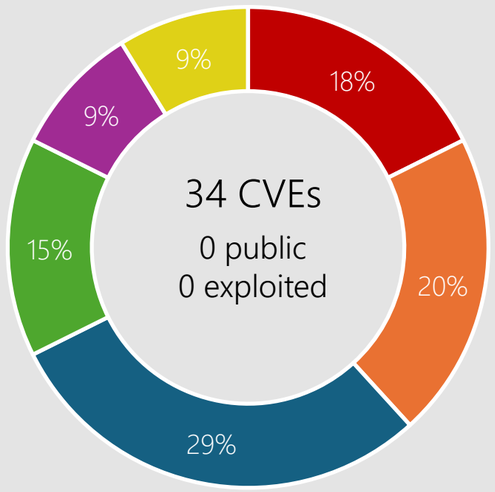
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

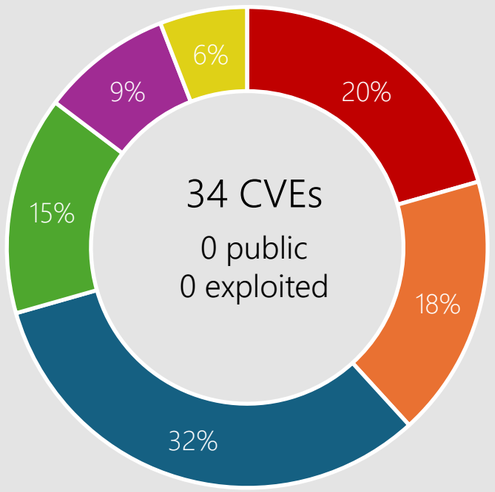
Affected Software

Windows 11
Windows 10
Server 2022
Server 2019

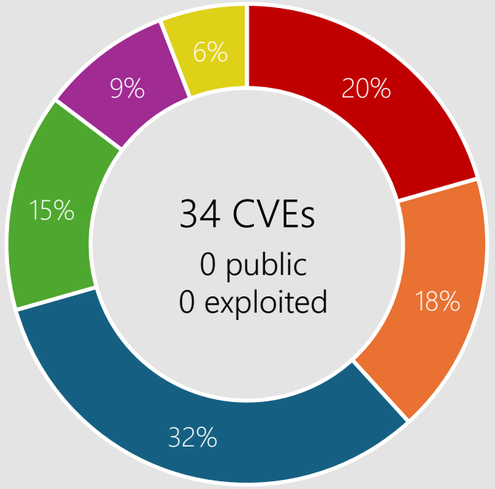
Windows 10



Windows 10 22H2

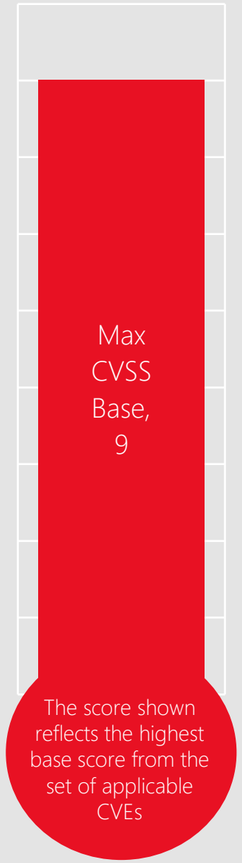


Windows 10 21H2



Windows 10 1809 & Windows Server 2019

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



Affected Components:

See appendix

CVE-2024-20654 ODBC Driver

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

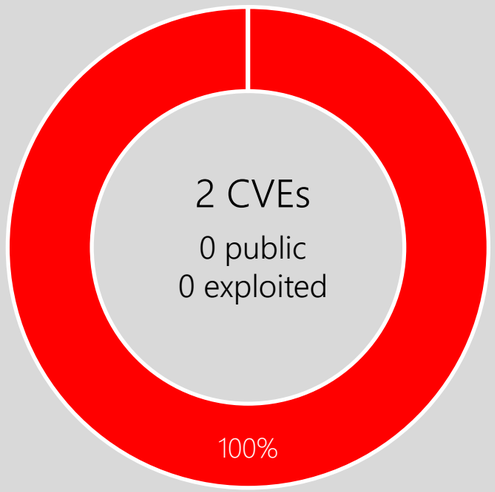
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 11
Windows 10
Server 2022
Server 2019
Server 2016

Microsoft Office



Microsoft Office-related software

Products:

Office 2019
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Office LTSC for Mac 2021
Office LTSC 2021
SharePoint Server Subscription Edition

CVE-2024-20677 Office

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
Office 2019
365 Apps Enterprise

CVE-2024-21318 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 Server 2019
SharePoint Enterprise Server 2016

Other Products

SQL Server

CVE-2024-0056 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 8.7
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: SQL Server 2022 (CU 10), SQL Server 2022 (GDR)

Developer Tools

Microsoft .NET Framework, .NET, Visual Studio

CVE-2024-0056 | Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass

Base CVSS: 8.7 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: High | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Microsoft .NET Framework (2.0, 3.5, 3.5.1, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1), .NET 6.0, 7.0, & 8.0, Visual Studio 2022

CVE-2024-0057 | .NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability

Base CVSS: 9.1 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Microsoft.NET Framework (2.0, 3.0, 3.5, 3.5.1, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1), NET 6.0, 7.0, & 8.0, Visual Studio 2022

CVE-2024-20672 | .NET Core and Visual Studio Denial of Service Vulnerability

Base CVSS: 7.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: .NET 6.0, 7.0

Developer Tools

Microsoft .NET Framework, .NET, Visual Studio, Microsoft Identity Model

CVE-2024-21312 | .NET Framework Denial of Service Vulnerability

Base CVSS: 7.5 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: None | **User Interaction Required**: None
Affected Products: Microsoft .NET Framework (3.5, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1)

CVE-2024-20656 | Visual Studio Elevation of Privilege Vulnerability

Base CVSS: 7.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Local | **Attack Complexity**: Low | **Privileges Required**: Low | **User Interaction Required**: None
Affected Products: Visual Studio 2015, 2019, 2022

CVE-2024-21319 | Microsoft Identity Denial of Service Vulnerability

Base CVSS: 6.8 | **Max Severity**: Important | **Public**: No | **Exploited**: No
Attack Vector: Network | **Attack Complexity**: Low | **Privileges Required**: High | **User Interaction Required**: None
Affected Products: Microsoft Identity Model, Microsoft Identity Model for Nuget, .NET 6.0, 7.0, 8.0, Visual Studio 2022

Other Products

Azure Storage Mover Agent

CVE-2024-20676 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
User Interaction: None
Products: Azure Storage Mover Agent.

Security Advisory Re-Release ADV190023

Summary

With the release of the January 9, 2024 security updates, the auditing changes added in August 2023 are now available on Windows Server 2019. You do not need to install MSIs or create policies as mentioned in Step 3 of Recommended Actions.

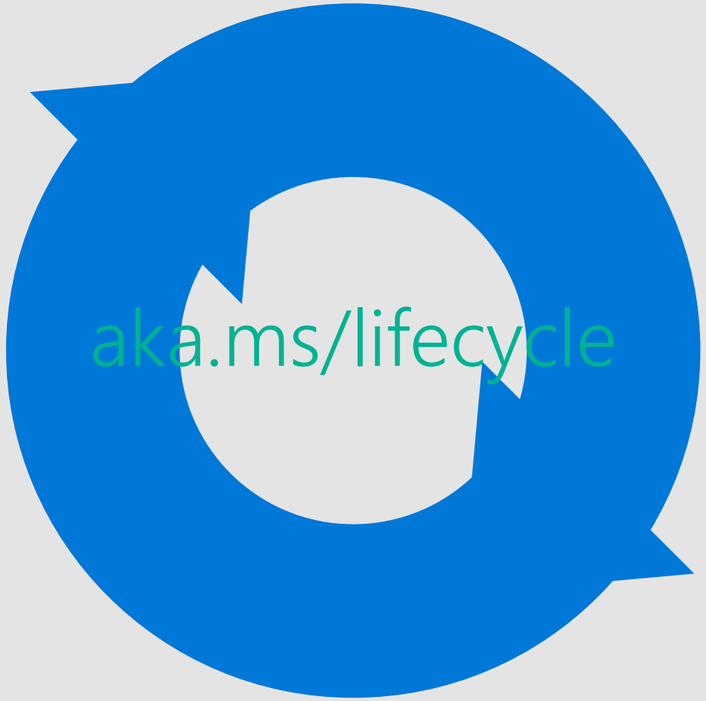
Suggested Actions:

Microsoft recommends that administrators configure LDAP signing and LDAP channel binding as recommended in Step One of the Executive Summary of this advisory and as described in detail in KB4520412: 2020 and 2023 LDAP channel binding and LDAP signing requirements for Windows.

https://msrc.microsoft.com/update-guide/vulnerability/ADV190023

Product Lifecycle Update

Nothing reaching end of support in January



Microsoft

Questions?

Appendix

Component Name	CVE's
Message Queuing	4
Cryptographic Services	2
Hyper-V	2
Libarchive	2
Message Queuing Client (MSMQC)	2
Online Certificate Status Protocol (OCSP)	2
Themes	2
Win32k	2
AllJoyn API	1
Bluetooth Driver	1
Cloud Files Mini Filter Driver	1
Common Log File System	1
Common Log File System Elevation of Privilege	1
CoreMessaging	1
Group Policy	1
HTML Platforms	1
Identity	1
Kerberos	1
Kernel	1
Kernel-Mode Driver	1
Local Security Authority Subsystem Service	1
Nearby Sharing	1
ODBC Driver	1
Office	1
Server Key Distribution Service	1
SharePoint Server	1
Subsystem for Linux	1
TCP/IP	1
Virtual Hard Disk	1
.Data.SqlClient and System.Data.SqlClient SQL Data Provider	1
.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass	1
.NET Core and Visual Studio	1
.NET Framework	1
Azure Storage Mover	1
BitLocker	1
Hypervisor-Protected Code Integrity (HVCI)	1
MITRE: CVE-2022-35737 SQLite allows an array-bounds overflow	1
NET, .NET Framework, and Visual Studio	1
Remote Desktop Client	1
Visual Studio	1