Microsoft

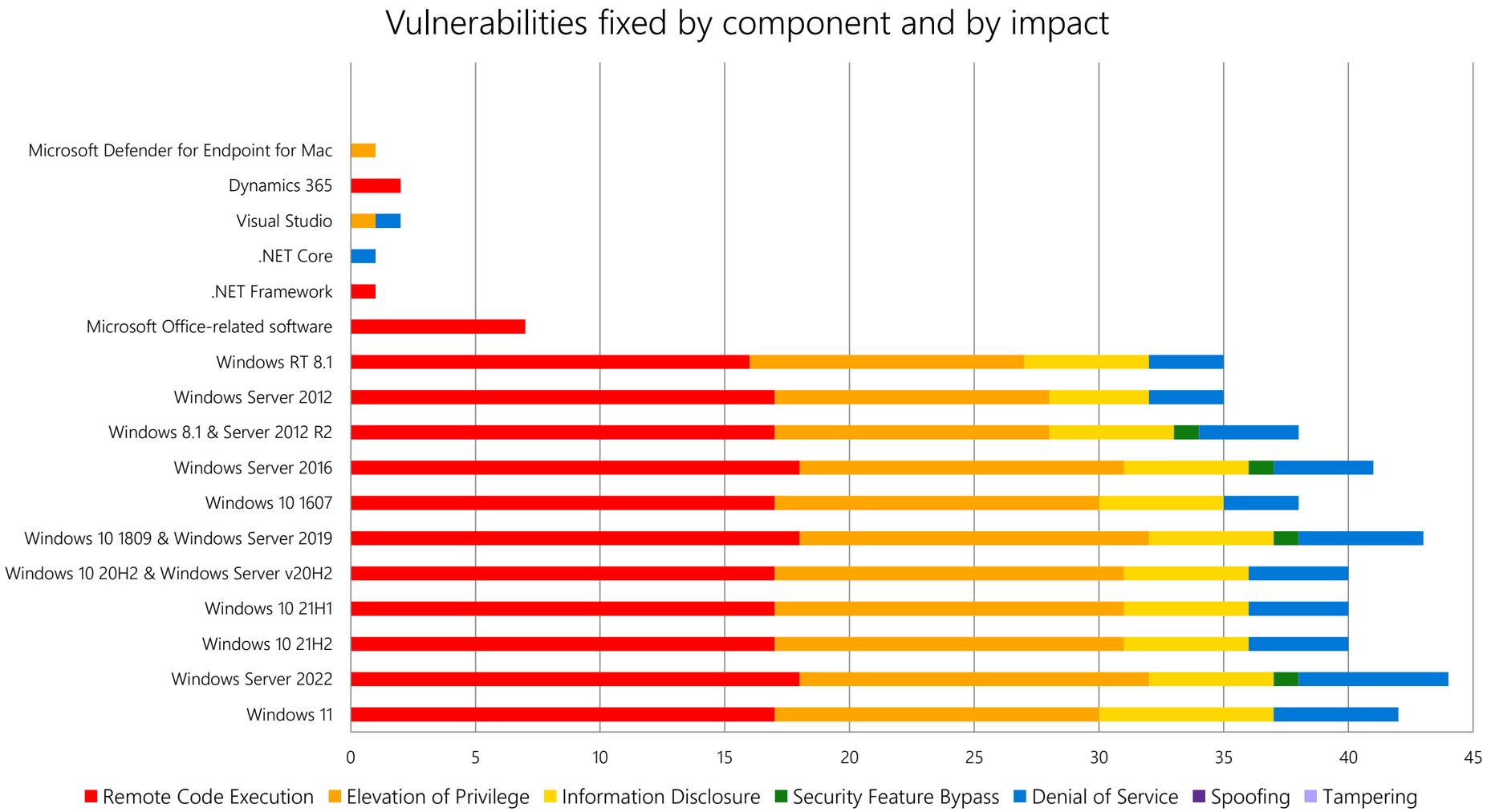
# Microsoft Security Release

September 13, 2022

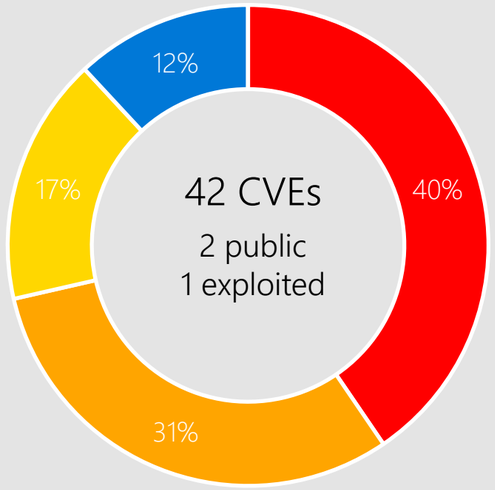
# Agenda

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

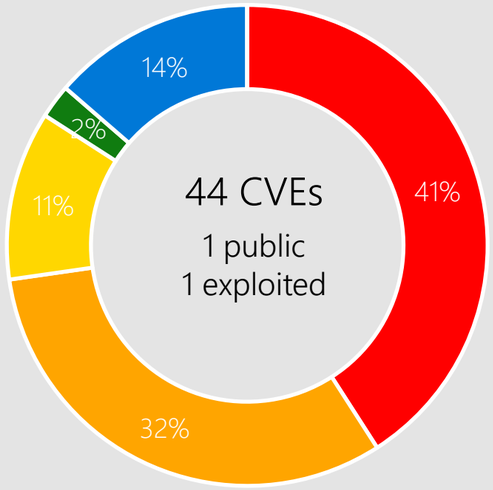
# Monthly Security Release Overview - September 2022



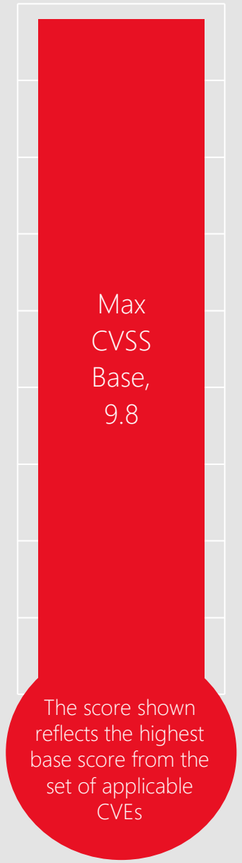
# Windows 11, Server 2022




Windows 11




Windows Server 2022




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

## Affected Components:

Please see Appendix for complete list.

# CVE-2022-34718 TCP/IP

## 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

Only systems with the IPSec service running are vulnerable to this attack.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# CVE-2022-37969 Common Log File System Driver

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly 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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-34721 Internet Key Exchange (IKE) Protocol Extensions

## 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

Microsoft has not identified any mitigating factors for this vulnerability.

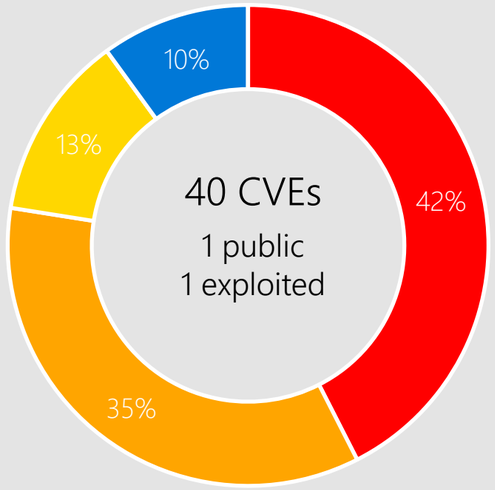
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

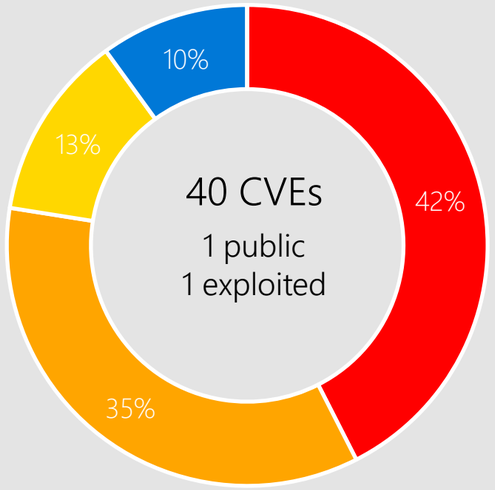
## Affected Software

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

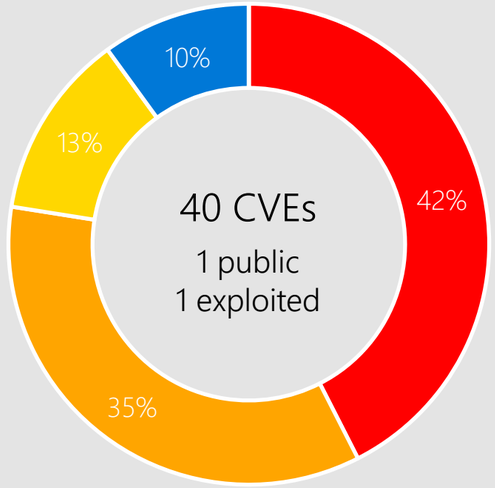
# Windows 10



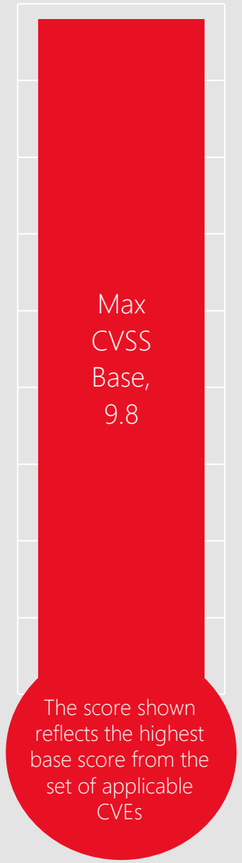

Windows 10 21H2




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:

Please see Appendix for complete list.

# CVE-2022-34731 OLE DB Provider for SQL

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

# CVE-2022-35841 Enterprise App Management Service

## 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
Server 2022
Server 2019
Windows 10
Server 2016

# CVE-2022-30196 Secure Channel

## Impact, Severity, Disclosure

Denial of Service | Important | Privately disclosed | No known exploits in the wild

## CVSSScoreMetrics

Base CVSS Score: 8.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

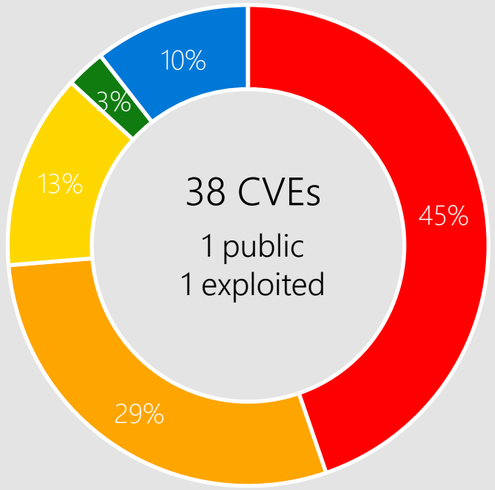
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

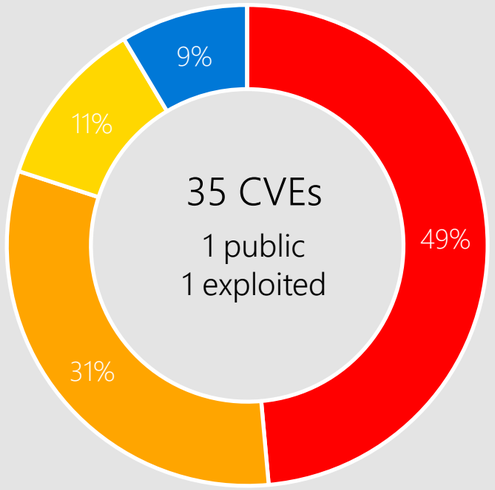
## Affected Software

Windows 11
Server 2022
Windows 10
Server 2019

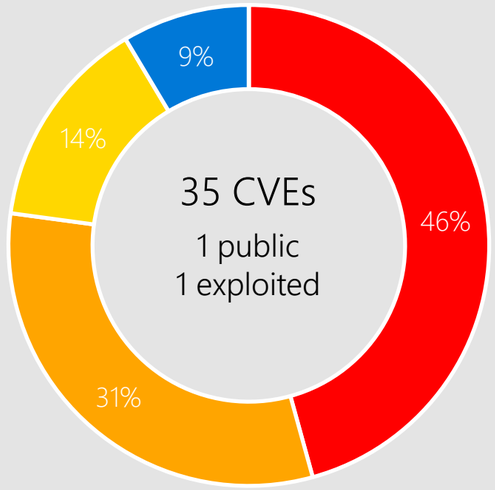
# Windows 8.1, Server 2012 R2, and Server 2012



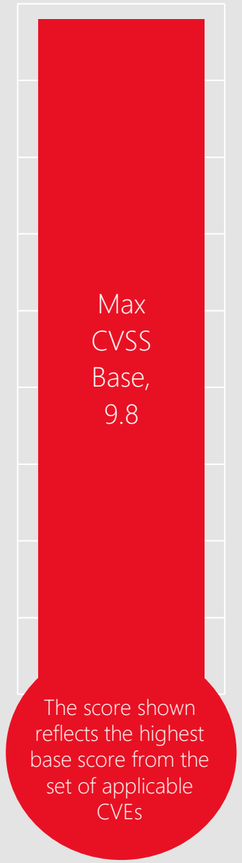

Windows 8.1 & Server 2012 R2




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:

Please see Appendix for complete list.

# CVE-2022-35830 Remote Procedure Call Runtime

## Impact, Severity, Disclosure

Remote Code Execution | Important | 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

Server 2022
Server 2019
Server 2016
Server 2012 R2
Server 2012

# CVE-2022-34726 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
- Server 2022
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-34729 GDI

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | No known exploits in the wild

## 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.

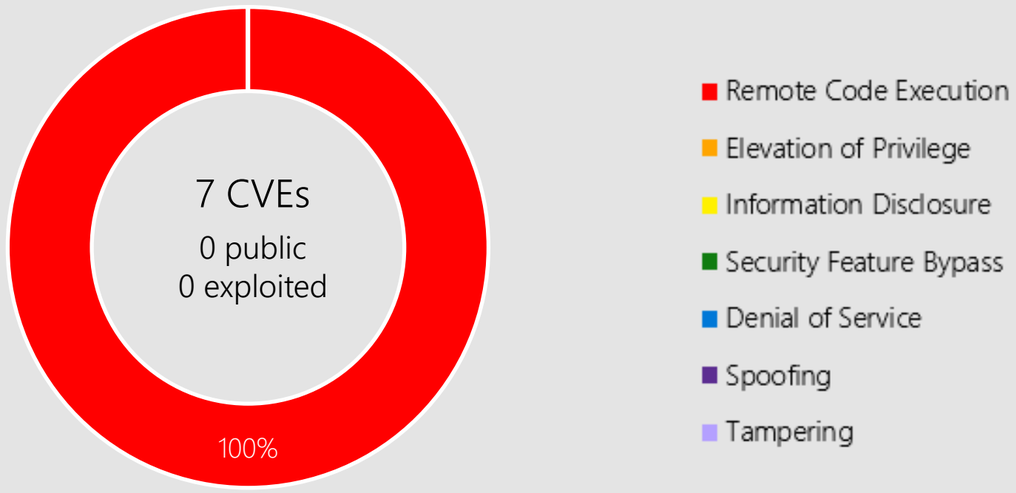
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# Microsoft Office




Microsoft Office-related software

## Products:

Office 2013/2016/2019
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps  Enterprise
Office LTSC 2021
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Server Subscription Edition Language Pack
Visio 2013
Visio 2016

# CVE-2022-37962 PowerPoint

## 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 2016
Office 2013
Office LTSC 2021
Office 2019
365 Apps  Enterprise

# CVE-2022-38008 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 Subscription Edition Language Pack
SharePoint Foundation 2013
SharePoint Enterprise Server 2016
SharePoint Enterprise Server 2013
SharePoint Server 2019

# Other Products

## Dynamics 365

CVE-2022-34700 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

CVE-2022-35805 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

# Other Products

## .NET Core and .NET 6.0

CVE-2022-38013 | 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: .NET Core 3.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 for Mac version 17.3, Visual Studio 2022 version 17.3, Visual Studio 2022 version 17.2, .NET 6.0.

# Other Products

## .NET Framework

CVE-2022-26929 | 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: **.NET Framework 3.5 AND 4.8** on Windows 11, Windows 10  20H2, Windows 10  1809, Server 2022, Server 2019,
**.NET Framework 3.5 AND 4.7.2** on Windows 10  1809, Server 2019,
**.NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2** on Windows 10  1607, Server 2016, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.8 on Server 2012
**.NET Framework 3.5** on Server 2012 R2, Windows 8.1, on Server 2012
**.NET Framework 3.5.1** on Server 2008 R2
**.NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2** on Windows 8.1, Server 2008 R2, Server 2012, Server 2012 R2
**.NET Framework 4.8.1** on Windows 10  21H1, Windows 10  21H2
**.NET Framework 3.5 AND 4.8.1** on Server 2022, Windows 11
**.NET Framework 4.8** on Windows 8.1, Server 2008 R2, Windows 10  21H1, Windows 10  21H2, Server 2016, Windows 10  1607

# Other Products

## Visual Studio

CVE-2022-38013 | 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: .NET Core 3.1, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2022 for Mac version 17.3, Visual Studio 2022 version 17.3, Visual Studio 2022 version 17.2, .NET 6.0.

CVE-2022-38020 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio Code.

# Other Products

## Microsoft Defender for Endpoint for Mac

CVE-2022-35828 | 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: Defender  Endpoint  for Mac.

# Other Products

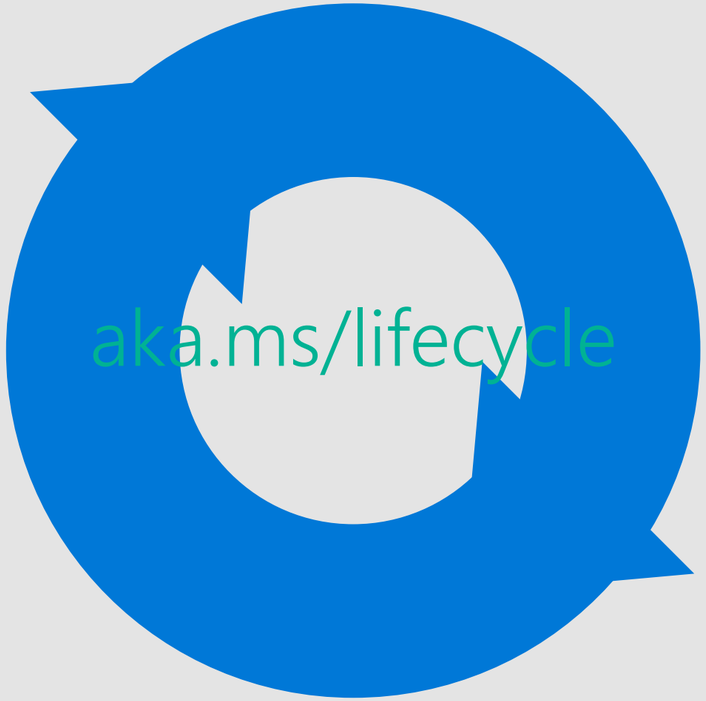
## Azure ARC & Azure Guest Configuration

CVE-2022-38007 | 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 ARC, Azure Guest Configuration

# Product Lifecycle Update

No products reaching end of support
in September




Latest Servicing Stack Updates

# Exchange Online Basic Authentication retirement is here

## September and October 2022

- If you have an Exchange Online tenant and need to keep using basic authentication for a protocol, you MUST opt out of basic authentication retirement during the month of September.
- All non-opted out protocols will be disabled for basic authentication with Exchange Online starting October 1, 2022.
- Opt-outs last until early January 2023.
- After October 1, you will have the ability to re-enable basic auth once, until early January 2023.
- See your tenant's Message Center for more information.

## Early January 2023

Exchange Online will *permanently* block connections utilizing basic authentication for the following protocols:

- MAPI, RPC, Offline Address Book (OAB), Exchange Web Services (EWS), POP, IMAP, Exchange ActiveSync (EAS), and Remote PowerShell.
- SMTP Auth (using basic auth) is *excluded* from retirement in January 2023. Date to be announced in the future.

http://aka.ms/exchangeteamblog

Microsoft

# Questions?

# Appendix

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2022-26928 | No | No | Photo Import API |
| CVE-2022-30170 | No | No | Credential Roaming Service |
| CVE-2022-30196 | No | No | Secure Channel |
| CVE-2022-33679 | No | No | Kerberos |
| CVE-2022-35803 | No | No | CLFS Driver |
| CVE-2022-35828 | No | No | Defender for Endpoint for Mac |
| CVE-2022-37964 | No | No | Kernel |
| CVE-2022-30200 | No | No | LDAP |
| CVE-2022-33647 | No | No | Kerberos |
| CVE-2022-35830 | No | No | RPCRuntime |
| CVE-2022-35831 | No | No | Remote Access Connection Manager |
| CVE-2022-35832 | No | No | Event Tracing |
| CVE-2022-35833 | No | No | Secure Channel |
| CVE-2022-35834 | No | No | OLE DB Provider for SQL Server |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2022-35835 | No | No | OLE DB Provider for SQL Server |
| CVE-2022-35836 | No | No | OLE DB Provider for SQL Server |
| CVE-2022-35837 | No | No | Graphics Component |
| CVE-2022-35840 | No | No | OLE DB Provider for SQL Server |
| CVE-2022-35841 | No | No | Enterprise App Management Service |
| CVE-2022-34718 | No | No | TCP/IP |
| CVE-2022-34719 | No | No | DFS |
| CVE-2022-34720 | No | No | Internet Key Exchange (IKE) |
| CVE-2022-34721 | No | No | Internet Key Exchange (IKE) |
| CVE-2022-34722 | No | No | Internet Key Exchange (IKE) |
| CVE-2022-34723 | No | No | DPAPI |
| CVE-2022-34724 | No | No | DNS Server |
| CVE-2022-34725 | No | No | ALPC |
| CVE-2022-34726 | No | No | ODBC Driver |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2022-34727 | No | No | ODBC Driver |
| CVE-2022-34728 | No | No | Graphics Component |
| CVE-2022-34729 | No | No | GDI |
| CVE-2022-34730 | No | No | ODBC Driver |
| CVE-2022-34731 | No | No | OLE DB Provider for SQL Server |
| CVE-2022-34732 | No | No | ODBC Driver |
| CVE-2022-34733 | No | No | OLE DB Provider for SQL Server |
| CVE-2022-34734 | No | No | ODBC Driver |
| CVE-2022-37954 | No | No | DirectX Graphics Kernel |
| CVE-2022-37955 | No | No | Group Policy |
| CVE-2022-37956 | No | No | Kernel |
| CVE-2022-38004 | No | No | Fax Service |
| CVE-2022-37957 | No | No | Kernel |
| CVE-2022-38005 | No | No | Print Spooler |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2022-38006 | No | No | Graphics Component |
| CVE-2022-38011 | No | No | Raw Image Extension |
| CVE-2022-37969 | No | Yes | Common Log File System Driver |
| CVE-2022-38019 | No | No | AV1 Video Extension |
| CVE-2022-35823 | No | No | SharePoint |
| CVE-2022-38008 | No | No | SharePoint Server |
| CVE-2022-38009 | No | No | SharePoint Server |
| CVE-2022-37961 | No | No | SharePoint Server |
| CVE-2022-38010 | No | No | Office Visio |
| CVE-2022-37962 | No | No | PowerPoint |
| CVE-2022-37963 | No | No | Office Visio |
| CVE-2022-26929 | No | No | .NET Framework |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2022-35805 | No | No | Dynamics 365 (on-premises) |
| CVE-2022-38013 | No | No | .NET Core and Visual Studio |
| CVE-2022-34700 | No | No | Dynamics 365 (on-premises) |
| CVE-2022-35838 | No | No | HTTP V3 |
| CVE-2022-37958 | No | No | SPNEGO Extended Negotiation (NEGOEX) Security Mechanism |
| CVE-2022-37959 | No | No | Network Device Enrollment Service (NDES) |
| CVE-2022-38007 | No | No | Azure Guest Configuration and Azure Arc-enabled servers |
| CVE-2022-23960 | Yes | No | Arm: CVE-2022-23960 Cache Speculation Restriction |
| CVE-2022-38020 | No | No | Visual Studio Code |

# CVE-2022-35803 Common Log File System Driver

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | No known exploits in the wild

## 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
- Server 2022
- Server 2022 Azure Edition Core Hotpatch
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-30200 Lightweight Directory Access Protocol (LDAP)

## 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

Windows 11
Server 2022
Server 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-35834 OLE DB Provider for SQL 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: 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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-35835 OLE DB Provider for SQL 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: 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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-35836 OLE DB Provider for SQL 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: 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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-35840 OLE DB Provider for SQL 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: 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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-34722 Internet Key Exchange (IKE) Protocol Extensions

## 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

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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-34727 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
- Server 2022
- Server 2022 Azure Edition Core Hotpatch
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-34730 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
- Server 2022
- Server 2022 Azure Edition Core Hotpatch
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-34733 OLE DB Provider for SQL 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: 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 2022 Azure Edition Core Hotpatch
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

# CVE-2022-34734 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
- Server 2022
- Server 2022 Azure Edition Core Hotpatch
- Server 2019
- Windows 10
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 8.1

# CVE-2022-38004 Fax Service

## 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

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

# CVE-2022-37957 Kernel

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | No known exploits in the wild

## 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
Server 2022
Server 2019
Windows 10
Server 2016

# CVE-2022-38011 Raw Image Extension

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 7.3 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: Low | User Interaction: Required

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

## Workarounds

## Affected Software

Raw Image Extension on Windows 10  21H2
Raw Image Extension on Windows 10
Raw Image Extension on Windows 10  1607
Raw Image Extension on Windows 10  20H2
Raw Image Extension on Windows 10  1809
HoloLens
Raw Image Extension on Windows 10  1809
Raw Image Extension on Windows 10  21H1
Raw Image Extension on Windows 11

# CVE-2022-38019 AV1 Video Extension

## 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

AV1 Video Extension

# CVE-2022-35823 SharePoint

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 8.1 | 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-2022-38009 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-2022-37961 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-2022-38010 Office Visio

## 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

Visio 2013
Visio 2016
Office LTSC 2021
Office 2019
365 Apps  Enterprise

# CVE-2022-37963 Office Visio

## 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
365 Apps  Enterprise
Office 2019

# CVE-2022-35823 SharePoint

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 8.1 | 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-2022-38008 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 Subscription Edition Language Pack
SharePoint Foundation 2013
SharePoint Enterprise Server 2016
SharePoint Enterprise Server 2013
SharePoint Server 2019

# CVE-2022-38009 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-2022-37961 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