Microsoft

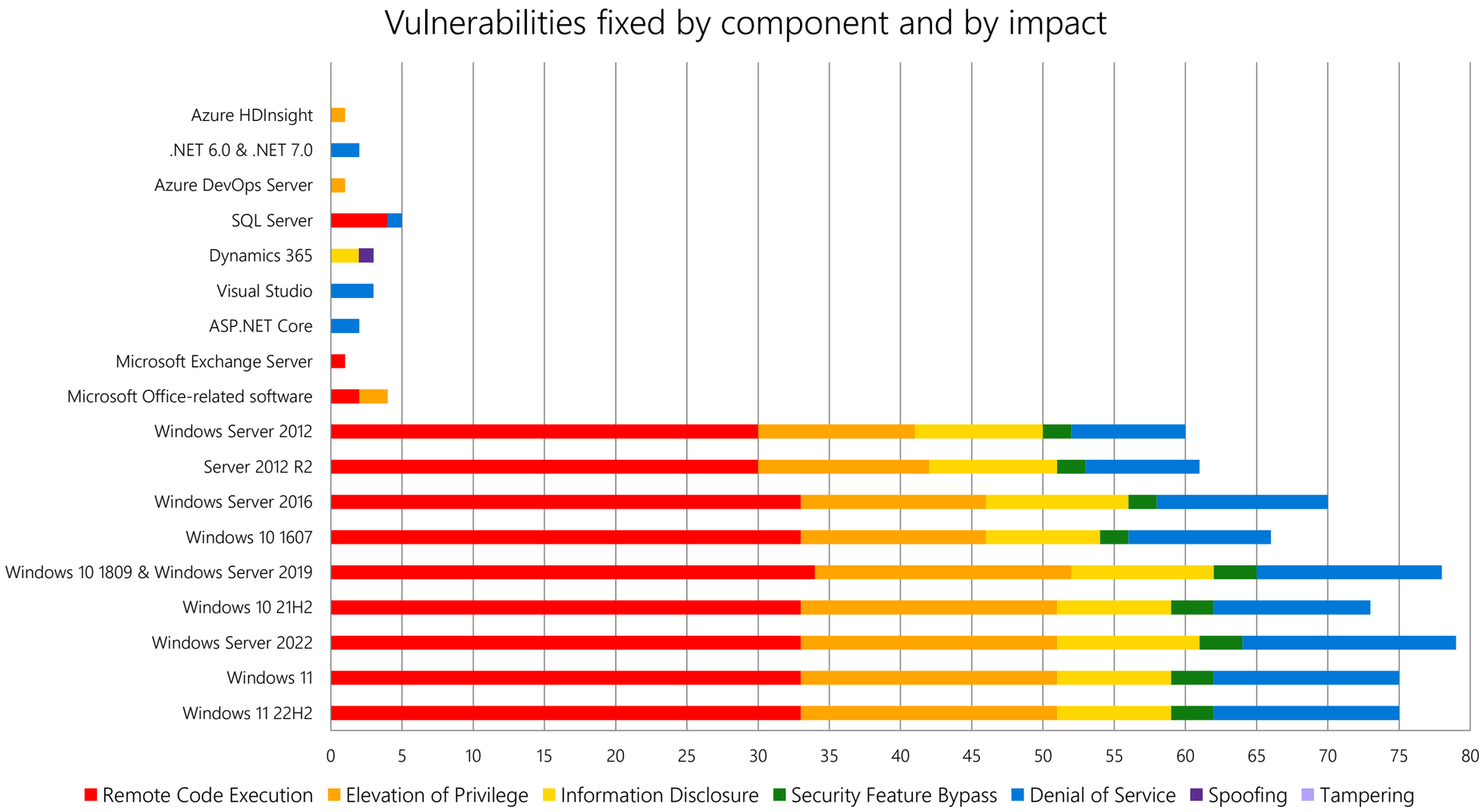
# Microsoft Security Release

October 10, 2023

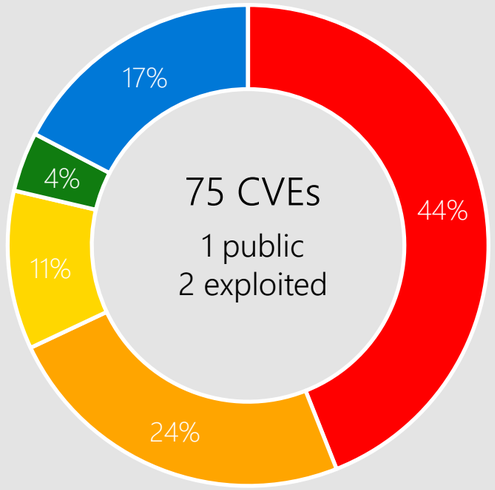
# Agenda

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

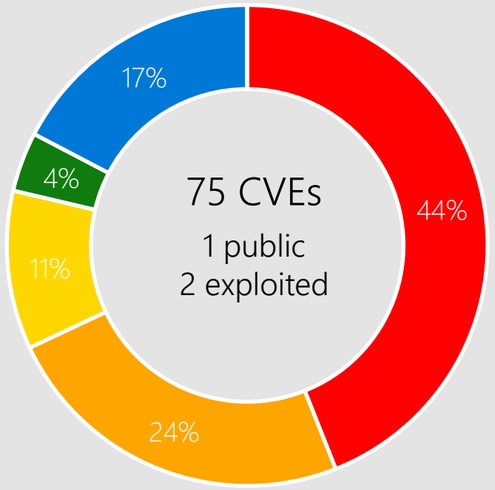
# Monthly Security Release Overview - October 2023



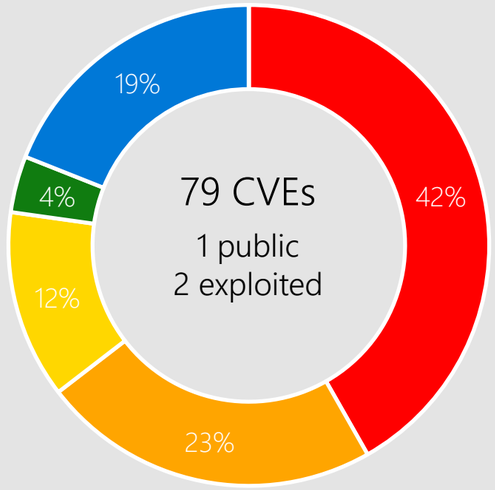
# Windows 11, Server 2022



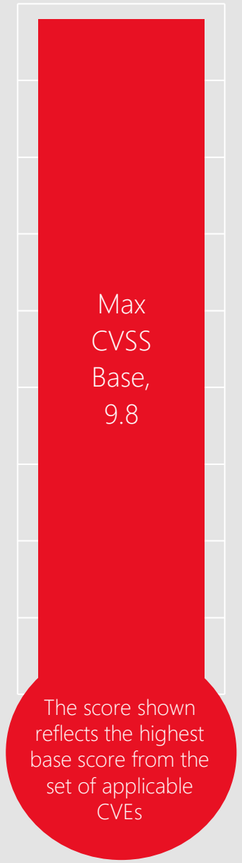

Windows 11 22H2




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-2023-36434 IIS Server

## Impact, Severity, Disclosure

Elevation of Privilege | Important | 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  22H2
- Windows 11 version 21H2
- Server 2022
- Server 2019
- Server 2016
- Server 2012 R2
- Server 2012
- Windows 10

# CVE-2023-35349 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

The Windows message queuing service, which is a Windows component, needs to be enabled for a system to be exploitable by this vulnerability. This feature can be added via the Control Panel.
You can check to see if there is a service running named Message Queuing and TCP port 1801 is listening on the machine.

## 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-2023-36577 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

Exploitation of this vulnerability requires an attacker to trick or convince the victim into connecting to their malicious server. If your environment only connects to known, trusted servers and there is no ability to reconfigure existing connections to point to another location (for example you use TLS encryption with certificate validation), the vulnerability cannot be exploited.

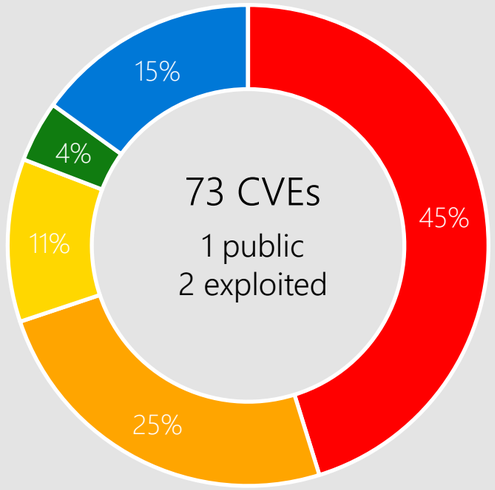
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

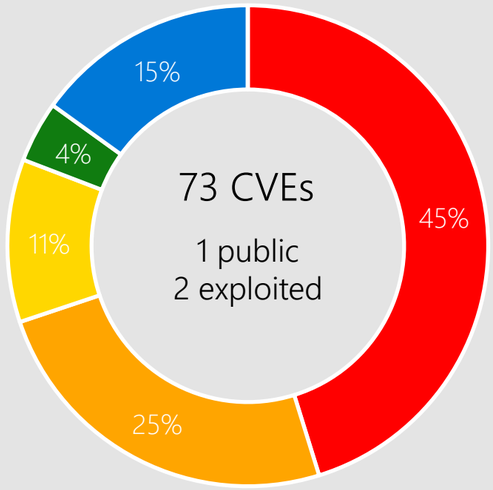
## Affected Software

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

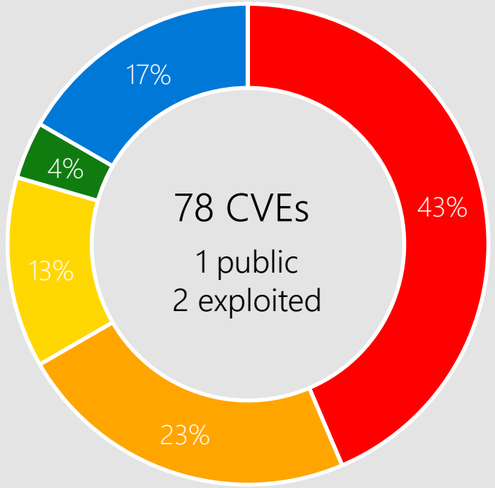
# Windows 10



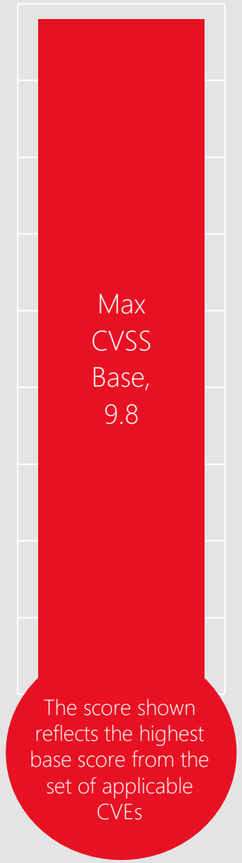

Windows 10 22H2




Windows 10 21H2




Windows 10 1809 & Windows Server 2019




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

## Affected Components:

See Appendix for details

# CVE-2023-36718 Virtual Trusted Platform Module

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: High | Privileges Required: Low | User Interaction: None

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

Windows 11  22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016

# CVE-2023-44487 HTTP/2

## Impact, Severity, Disclosure

Denial of Service | Important | Privately disclosed | Exploitation Detected

## CVSSScoreMetrics

See CVE-2023-44487 for details

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

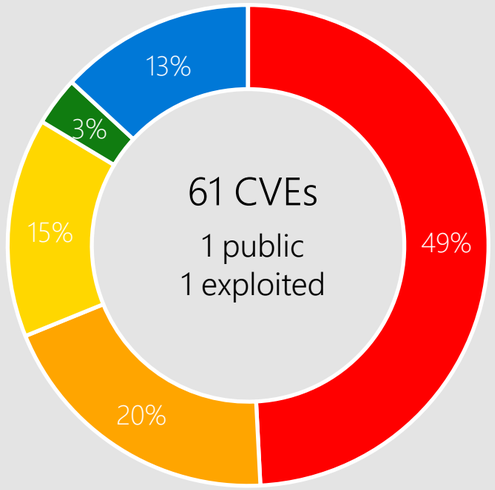
## Workarounds

Disable HTTP/2 protocol. See CVE entry for details.

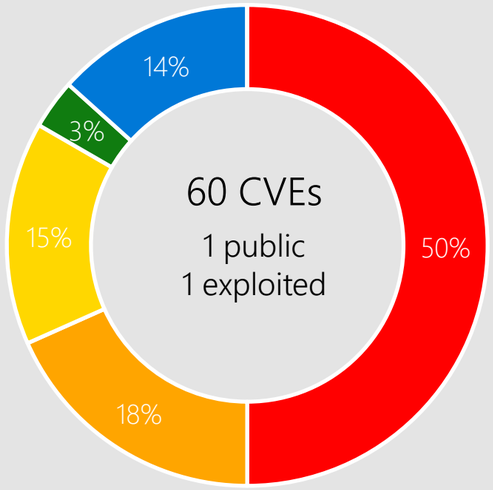
## Affected Software

Windows 11  22H2
Windows 11 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016

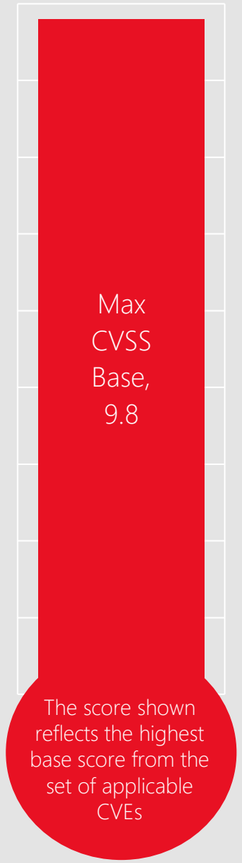
# Server 2012 R2, and Server 2012




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-2023-41765 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

# CVE-2023-36563 WordPad

## Impact, Severity, Disclosure

Information Disclosure | Important | Publicly Disclosed | Exploitation Detected

## CVSSScoreMetrics

Base CVSS Score: 6.5 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

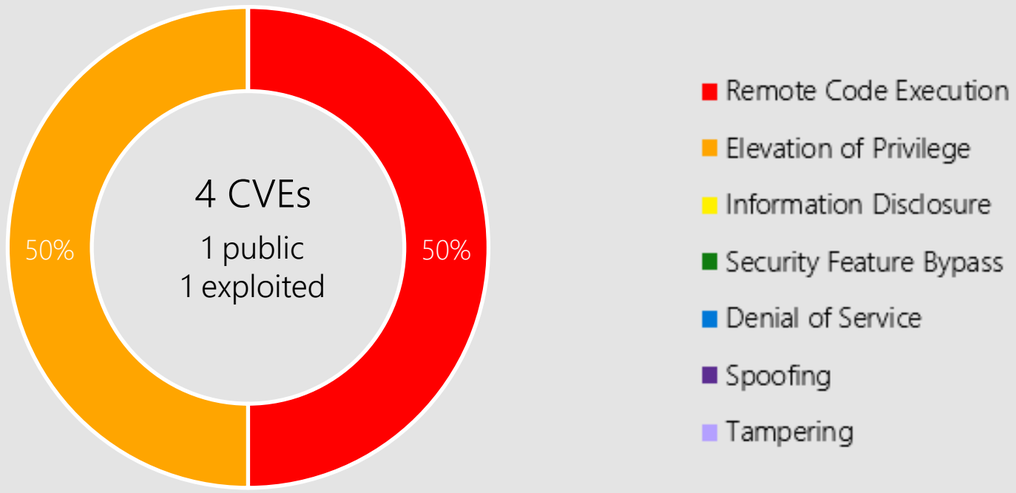
## Workarounds

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
365 Apps Enterprise
Office Android
Office Universal
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Skype Business Server 2015 CU13
Skype Business Server 2019 CU6
Skype Business Server 2019 CU7

# CVE-2023-36569 Office

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 8.4 | Attack Vector: Local | 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

Office LTSC 2021
365 Apps  Enterprise
Office 2019

# CVE-2023-41763 Skype for Business

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Publicly Disclosed | Exploitation Detected

## CVSSScoreMetrics

Base CVSS Score: 5.3 | 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

Skype Business Server 2019 CU6

# Other Products

## Exchange Server

CVE-2023-36778 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 13.

# Other Products

## SQL Server

### CVE-2023-36730 | 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: ODBC Driver 18 SQL Server on Linux, ODBC Driver 18 SQL Server on Windows, ODBC Driver 17 SQL Server on for MacOS, SQL Server 2019 (CU 22), SQL Server 2022 (CU 8), ODBC Driver 18 SQL Server on for MacOS, ODBC Driver 17 SQL Server, SQL Server 2022 (GDR), SQL Server 2019 (GDR), ODBC Driver 17 SQL Server on Linux, ODBC Driver 17 SQL Server on Windows, ODBC Driver 18 SQL Server.

### CVE-2023-36785 | 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: ODBC Driver 18 SQL Server on Linux, ODBC Driver 18 SQL Server on Windows, ODBC Driver 17 SQL Server on for MacOS, SQL Server 2022 (CU 8), SQL Server 2019 (CU 22), ODBC Driver 18 SQL Server on for MacOS, ODBC Driver 18 SQL Server, SQL Server 2022 (GDR), SQL Server 2019 (GDR), ODBC Driver 17 SQL Server on Linux, ODBC Driver 17 SQL Server on Windows, ODBC Driver 17 SQL Server.

# Other Products

## SQL Server

CVE-2023-36417 | 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: OLE DB Driver 18 SQL Server, SQL Server 2022 (CU 8), SQL Server 2019 (CU 22), SQL Server 2019 (GDR), SQL Server 2022 (GDR), OLE DB Driver 19 SQL Server.

CVE-2023-36420 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: ODBC Driver 18 SQL Server on Linux, ODBC Driver 18 SQL Server on Windows, ODBC Driver 17 SQL Server on for MacOS, SQL Server 2019 (CU 22), SQL Server 2022 (CU 8), ODBC Driver 18 SQL Server on for MacOS, ODBC Driver 17 SQL Server on Linux, ODBC Driver 18 SQL Server, SQL Server 2022 (GDR), SQL Server 2019 (GDR), ODBC Driver 17 SQL Server on Windows, SQL Server 2022 (CU 5), ODBC Driver 17 SQL Server.

# Other Products

## SQL Server

CVE-2023-36728 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 5.5
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: OLE DB Driver 18 SQL Server, ODBC Driver 17 SQL Server on Windows, OLE DB Driver 19 SQL Server, ODBC Driver 18 SQL Server, ODBC Driver 17 SQL Server, ODBC Driver 18 SQL Server on Linux, ODBC Driver 18 SQL Server on for MacOS, ODBC Driver 18 SQL Server on Windows, ODBC Driver 17 SQL Server on Linux, ODBC Driver 17 SQL Server on for MacOS, SQL Server 2014 (GDR), SQL Server 2014 (CU 4), SQL Server 2017 (GDR), SQL Server 2019 (CU 22), SQL Server 2022 (CU 8), SQL Server 2017 (CU 31), SQL Server 2022 (GDR), SQL Server 2016 Azure Connectivity Pack, SQL Server 2019 (GDR), SQL Server 2016 (GDR).

# Other Products

## Dynamics 365

CVE-2023-36416 | 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 9.0, Dynamics 365 (on-premises) version 9.1.

CVE-2023-36433 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 6.5
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

## Dynamics 365

CVE-2023-36429 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 6.5
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.

# Developer Tools

## .NET 6.0, .NET 7.0, ASP.NET Core 6.0, ASP.NET Core 7.0, Visual Studio 2022

### CVE-2023-44487 | MITRE: HTTP/2 Rapid Reset Attack Denial of Service

Severity: Important | Public: No | Exploited: Yes
CVSS Details: see Mitre CVE
Affected Products: .NET (6.0 & 7.0), ASP.NET Core (6.0 & 7.0), Visual Studio 2022

---

### CVE-2023-38171 | Microsoft QUIC Denial of Service Vulnerability

CVSS: 7.5 | Severity: Important | Public: No | Exploited: No
Attack Vector: Network | Complexity: Low | Privileges Required: None | User Interaction: None
Affected Products: .NET 7.0, Visual Studio 2022

---

### CVE-2023-36435 | Microsoft QUIC Denial of Service Vulnerability

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

# Developer Tools

## Microsoft Common Data Model SDK

### CVE-2023-36566 | Microsoft Common Data Model SDK Denial of Service Vulnerability

CVSS: 6.5 | Severity: Important | Public: No | Exploited: No

Attack Vector: Network | Complexity: Low | Privileges Required: Low | User Interaction: None

Affected Products: Microsoft Common Data Model SDK

## Azure DevOps Server

### CVE-2023-36561 | Azure DevOps Server Elevation of Privilege Vulnerability

CVSS: 7.3 | Severity: Important | Public: No | Exploited: No

Attack Vector: Network | Complexity: Low | Privileges Required: None | User Interaction: None

Affected Products: Azure DevOps Server 2020.0.2, Azure DevOps Server 2020.1.2, Azure DevOps Server 2022.0.1.

# Other Products

## Azure HDInsight

CVE-2023-36419 | Important | 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: Azure HDInsight.

# Other Products

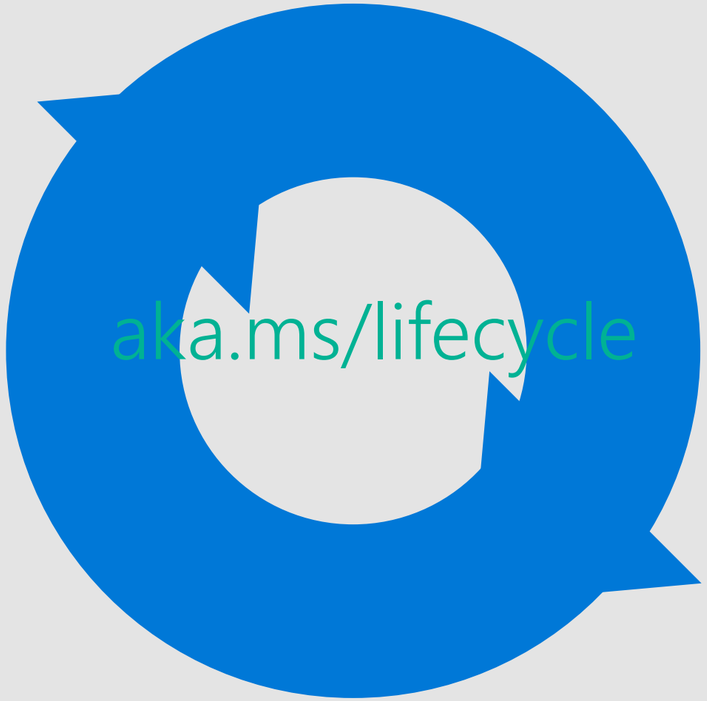
## Azure

CVE-2023-36737 : Azure Network Watcher VM Extension
CVE-2023-36418 AzureOS GUIX Studio, AzureOS GUIX Studio Installer Application
CVE-2023-36414/36415 Azure Identity SDK

# Product Lifecycle Update

Products reaching end of support

Windows Server 2012/2012R2




Modern policy- end of servicing

Windows 11 Home and Pro, Version 21H2

Microsoft Configuration Manager, Version 2203

Dynamics 365 Business Central on-premises (Modern Policy), 2022 release wave 1, version 20.x

Microsoft

# Questions?

# Appendix

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-35349 | No | No | Message Queuing |
| CVE-2023-36902 | No | No | Runtime |
| CVE-2023-41765 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41766 | No | No | Client Server Run-time Subsystem (CSRSS) |
| CVE-2023-41767 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41768 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41769 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41770 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41771 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41772 | No | No | Win32k |
| CVE-2023-41773 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-41774 | No | No | Layer 2 Tunneling Protocol |
| CVE-2023-36732 | No | No | Win32k |
| CVE-2023-36731 | No | No | Win32k |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-36729 | No | No | Named Pipe File System |
| CVE-2023-36726 | No | No | IKE |
| CVE-2023-36725 | No | No | Kernel |
| CVE-2023-36724 | No | No | Power Management Service |
| CVE-2023-36723 | No | No | Container Manager Service |
| CVE-2023-36721 | No | No | Error Reporting Service |
| CVE-2023-36720 | No | No | Mixed Reality Developer Tools |
| CVE-2023-36718 | No | No | Virtual TPM |
| CVE-2023-36717 | No | No | Virtual TPM |
| CVE-2023-36713 | No | No | Common Log File System Driver |
| CVE-2023-36712 | No | No | Kernel |
| CVE-2023-36711 | No | No | Runtime C++ Template Library |
| CVE-2023-36710 | No | No | Media Foundation Core |
| CVE-2023-36709 | No | No | AllJoyn API |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-36707 | No | No | Deployment Services |
| CVE-2023-36706 | No | No | Deployment Services |
| CVE-2023-36704 | No | No | Setup Files Cleanup |
| CVE-2023-36703 | No | No | DHCP Server Service |
| CVE-2023-36702 | No | No | DirectMusic |
| CVE-2023-36701 | No | No | Resilient File System (ReFS) |
| CVE-2023-36698 | No | No | Kernel |
| CVE-2023-36697 | No | No | Message Queuing |
| CVE-2023-36606 | No | No | Message Queuing |
| CVE-2023-36605 | No | No | Named Pipe Filesystem |
| CVE-2023-36603 | No | No | TCP/IP |
| CVE-2023-36602 | No | No | TCP/IP |
| CVE-2023-36596 | No | No | Remote Procedure Call |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-36594 | No | No | Graphics Component |
| CVE-2023-36593 | No | No | Message Queuing |
| CVE-2023-36592 | No | No | Message Queuing |
| CVE-2023-36591 | No | No | Message Queuing |
| CVE-2023-36590 | No | No | Message Queuing |
| CVE-2023-36589 | No | No | Message Queuing |
| CVE-2023-36585 | No | No | Active Template Library |
| CVE-2023-36584 | No | No | Mark of the Web |
| CVE-2023-36583 | No | No | Message Queuing |
| CVE-2023-36582 | No | No | Message Queuing |
| CVE-2023-36581 | No | No | Message Queuing |
| CVE-2023-36579 | No | No | Message Queuing |
| CVE-2023-36578 | No | No | Message Queuing |
| CVE-2023-36576 | No | No | Kernel |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-36575 | No | No | Message Queuing |
| CVE-2023-36574 | No | No | Message Queuing |
| CVE-2023-36573 | No | No | Message Queuing |
| CVE-2023-36572 | No | No | Message Queuing |
| CVE-2023-36571 | No | No | Message Queuing |
| CVE-2023-36570 | No | No | Message Queuing |
| CVE-2023-36567 | No | No | Deployment Services |
| CVE-2023-36564 | No | No | Search |
| CVE-2023-36557 | No | No | PrintHTML API |
| CVE-2023-36438 | No | No | TCP/IP |
| CVE-2023-36434 | No | No | IIS Server |
| CVE-2023-36431 | No | No | Message Queuing |
| CVE-2023-29348 | No | No | Remote Desktop Gateway (RD Gateway) |
| CVE-2023-38166 | No | No | Layer 2 Tunneling Protocol |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-38159 | No | No | Graphics Component |
| CVE-2023-36790 | No | No | RDP Encoder Mirror Driver |
| CVE-2023-36776 | No | No | Win32k |
| CVE-2023-36743 | No | No | Win32k |
| CVE-2023-36565 | No | No | Office Graphics |
| CVE-2023-36436 | No | No | MSHTML Platform |
| CVE-2023-41763 | Yes | Yes | Skype for Business |
| CVE-2023-36569 | No | No | Office |
| CVE-2023-36568 | No | No | Office Click-To-Run |
| CVE-2023-36563 | Yes | Yes | WordPad |
| CVE-2023-36789 | No | No | Skype for Business |
| CVE-2023-36786 | No | No | Skype for Business |
| CVE-2023-36780 | No | No | Skype for Business |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-38171 | No | No | QUIC |
| CVE-2023-36737 | No | No | Azure Network Watcher VM Agent |
| CVE-2023-36730 | No | No | SQL ODBC Driver |
| CVE-2023-36728 | No | No | SQL Server |
| CVE-2023-36722 | No | No | AD Domain Services |
| CVE-2023-36598 | No | No | WDAC ODBC Driver |
| CVE-2023-36577 | No | No | WDAC OLE DB provider for SQL Server |
| CVE-2023-36561 | No | No | Azure DevOps Server |
| CVE-2023-36435 | No | No | QUIC |
| CVE-2023-36433 | No | No | Dynamics 365 (On-Prem) |
| CVE-2023-36429 | No | No | Dynamics 365 (On-Prem) |
| CVE-2023-36420 | No | No | SQL ODBC Driver |
| CVE-2023-36419 | No | No | Azure HDInsight Apache Oozie Workflow Scheduler |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-36417 | No | No | SQL OLE DB |
| CVE-2023-44487 | No | Yes | MITRE: CVE-2023-44487 HTTP/2 Rapid Reset Attack |
| CVE-2023-36785 | No | No | SQL ODBC Driver |
| CVE-2023-36778 | No | No | Exchange Server |
| CVE-2023-36566 | No | No | Common Data Model SDK |
| CVE-2023-36418 | No | No | Azure RTOS GUIX Studio |
| CVE-2023-36416 | No | No | Dynamics 365 (on-prem) |
| CVE-2023-36415 | No | No | Azure Identity SDK |
| CVE-2023-36414 | No | No | Azure Identity SDK |
| | | | |
| | | | |
| | | | |
| | | | |