Microsoft

# Microsoft Security Release

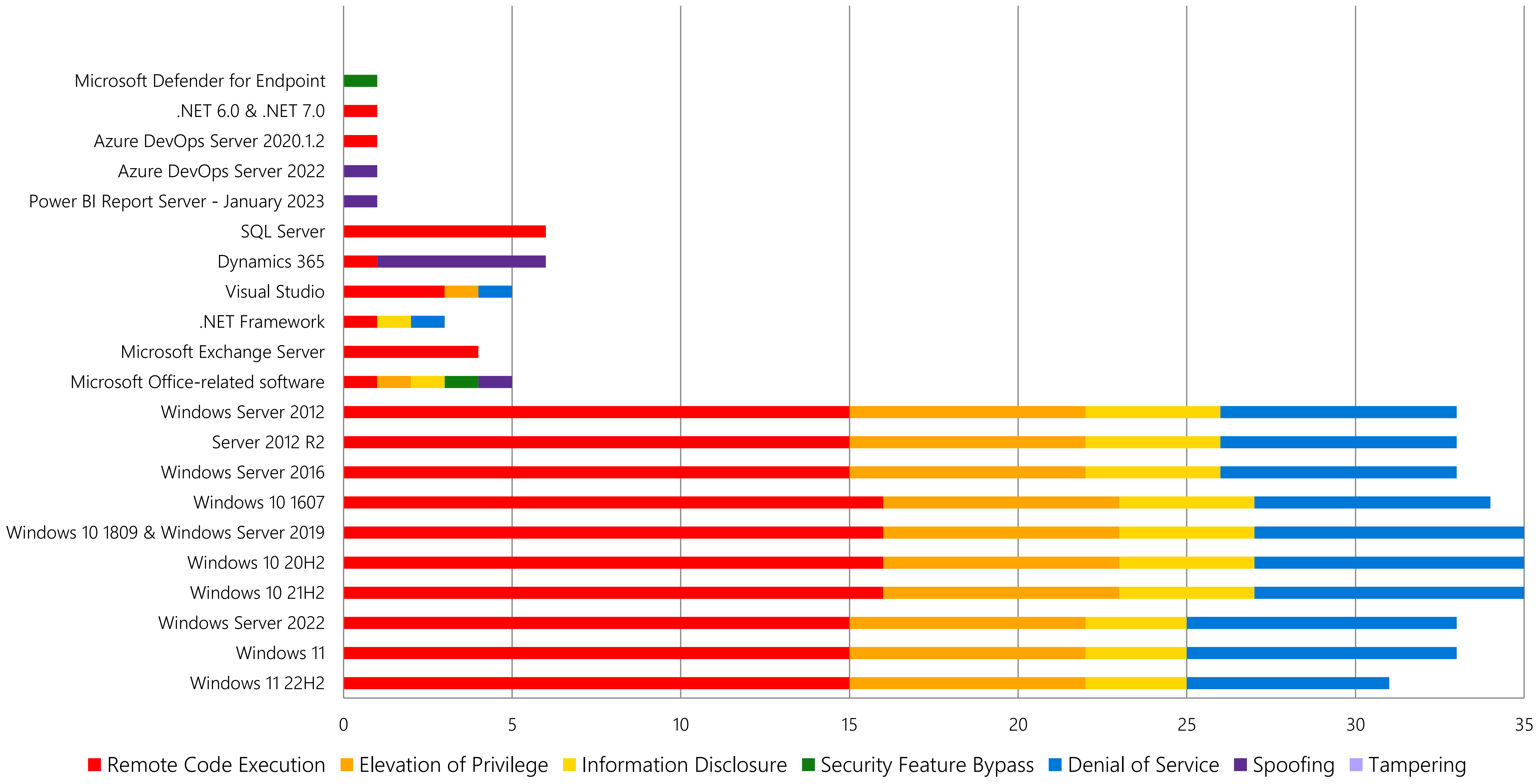
February 14, 2023

# Agenda

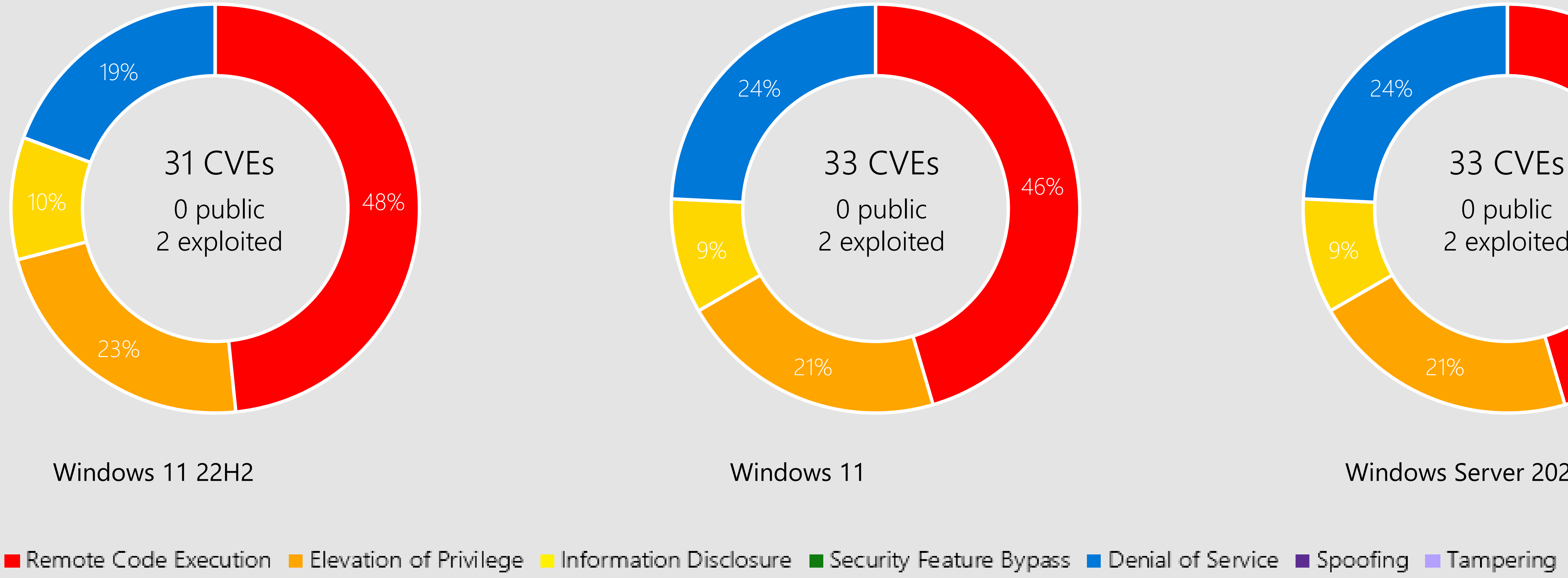
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

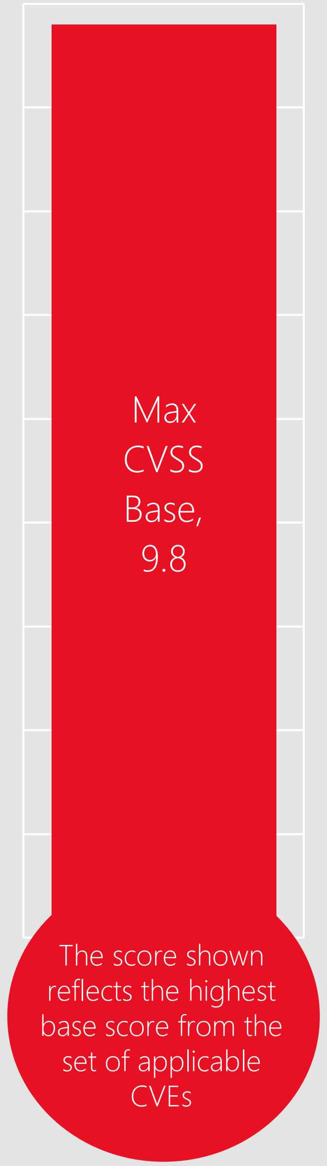
# Monthly Security Release Overview - February 2023

## Vulnerabilities fixed by component and by impact



# Windows 11, Server 2022





The score shown reflects the highest base score from the set of applicable CVEs

## Affected Components:

- Active Directory Domain Services API
- Common Log File System Driver
- Distributed File System (DFS)
- Fax Service
- Graphics Component
- HTTP.sys
- iSCSI Discovery Service
- iSCSI Service
- Kerberos
- Media
- MSHTML Platform
- NT OS Kernel
- ODBC Driver
- PostScript Printer Driver
- Protected Extensible Authentication Protocol (PEAP)

# CVE-2023-21689 PEAP

## 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 Protected Extensible Authentication Protocol (PEAP) is only negotiated with the client if NPS is running on the Windows Server and has a network policy configured that allows PEAP.

## More Information

[Configure the New Wireless Network Policy]()
[Configure Network Policies]()

## Affected Software

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

# CVE-2023-23376 Common Log File System Driver

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

## CVSSScoreMetrics

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

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# CVE-2023-21823 Graphics Component

## Impact, Severity, Disclosure

Elevation of Privilege | Important | Privately disclosed | Exploitation Detected

## CVSSScoreMetrics

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

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

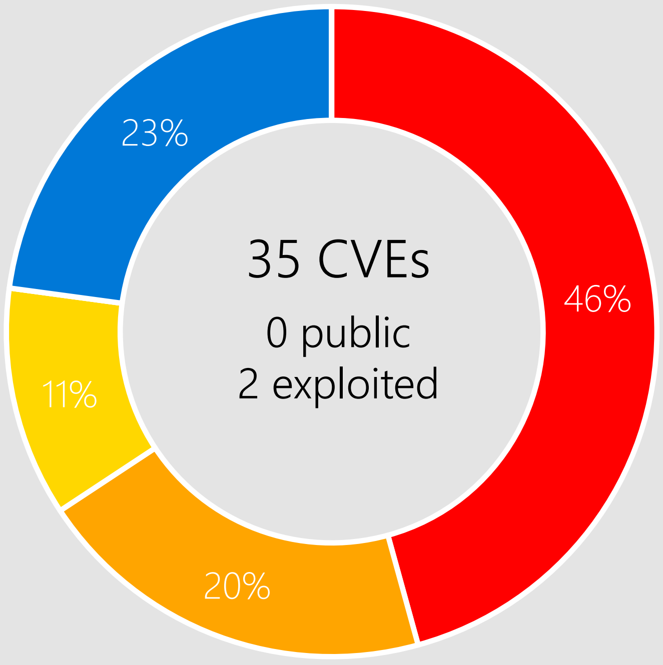
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

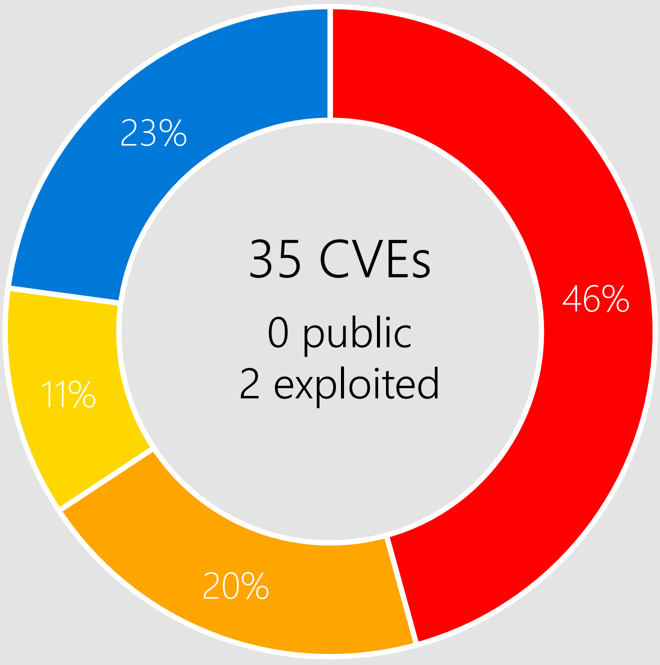
## Affected Software

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

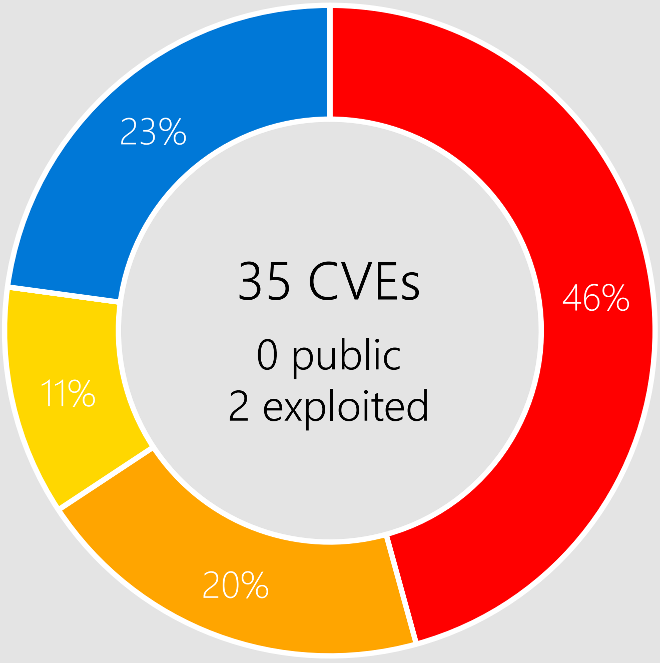
# Windows 10



Windows 10 21H2

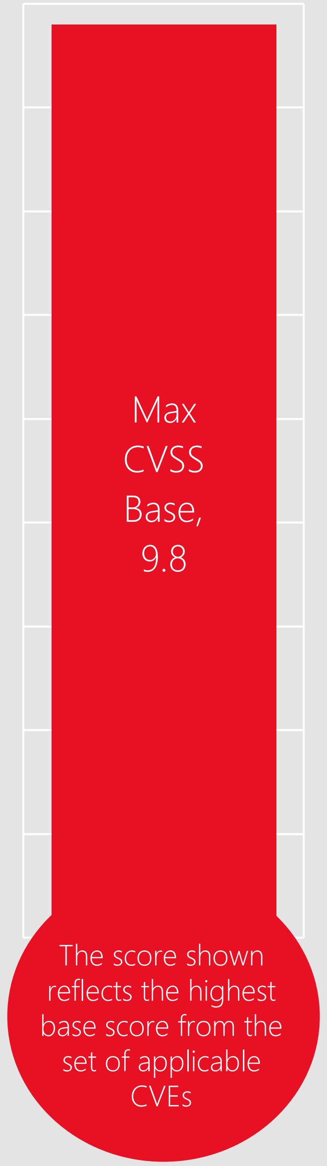


Windows 10 20H2



Windows 10 1809 & Windows Server 2019

🟥 Remote Code Execution 🟧 Elevation of Privilege 🟨 Information Disclosure 🟩 Security Feature Bypass 🟦 Denial of Service 🟪 Spoofing 🟪 Tampering



Max CVSS Base, 9.8

The score shown reflects the highest base score from the set of applicable CVEs

## Affected Components:

Active Directory Domain Services API
Common Log File System Driver
Distributed File System (DFS)
Fax Service
Graphics Component
Internet Storage Name Service (iSNS) Server
iSCSI Discovery Service
iSCSI Service
Kerberos
Media
MSHTML Platform
NT OS Kernel
ODBC Driver
PostScript Printer Driver
Protected Extensible Authentication Protocol (PEAP)

# CVE-2023-21803 iSCSI Discovery Service

## 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

By default, the iSCSI Initiator client application is disabled, in this state an attacker cannot exploit this vulnerability. For a system to be vulnerable, the iSCSI Initiator client application would need to be enabled.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

Windows 10

# CVE-2023-21684 PS Printer 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: Low | User Interaction: None

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# CVE-2023-21799 WDAC OLE DB Provider

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

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

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

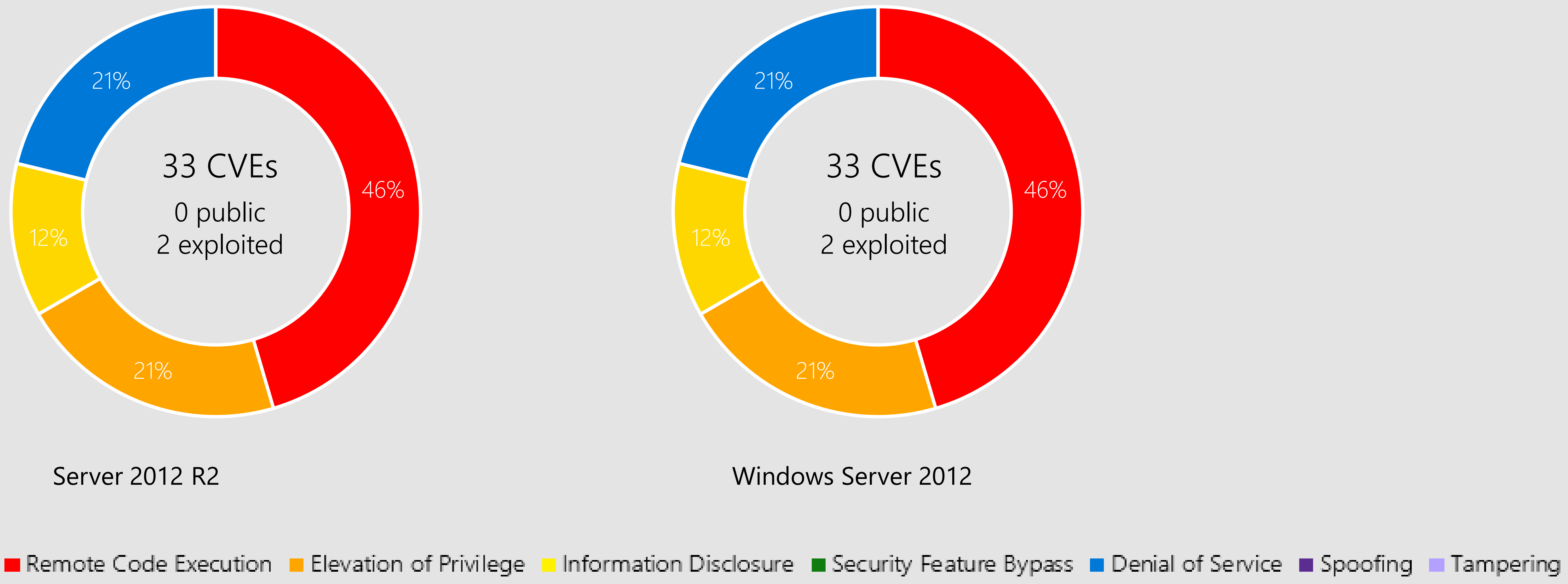
## Workarounds

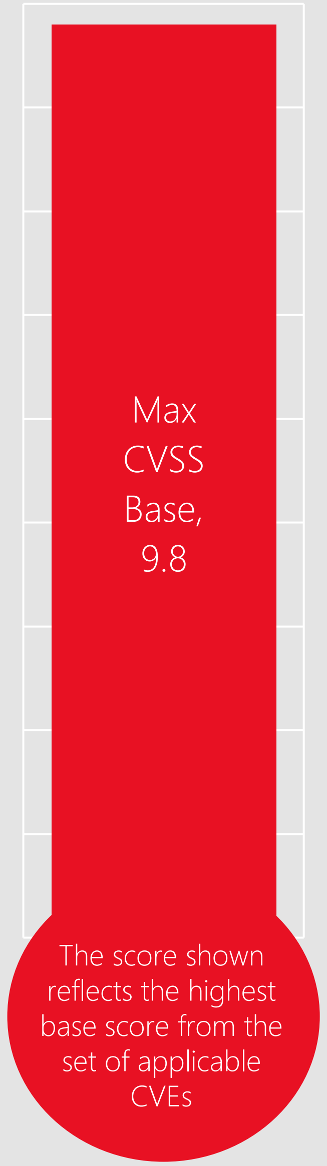
Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# Server 2012 R2, and Server 2012





The score shown reflects the highest base score from the set of applicable CVEs

## Affected Components:

Active Directory Domain Services API
Common Log File System Driver
Distributed File System (DFS)
Fax Service
Graphics Component
Internet Storage Name Service (iSNS) Server
iSCSI Discovery Service
iSCSI Service
Kerberos
Media
MSHTML Platform
NT OS Kernel
ODBC Driver
PostScript Printer Driver
Protected Extensible Authentication Protocol (PEAP)

# CVE-2023-21797 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 version 21H2
Server 2022
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012

# CVE-2023-21817 Kerberos

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

# CVE-2023-21813 Secure Channel

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

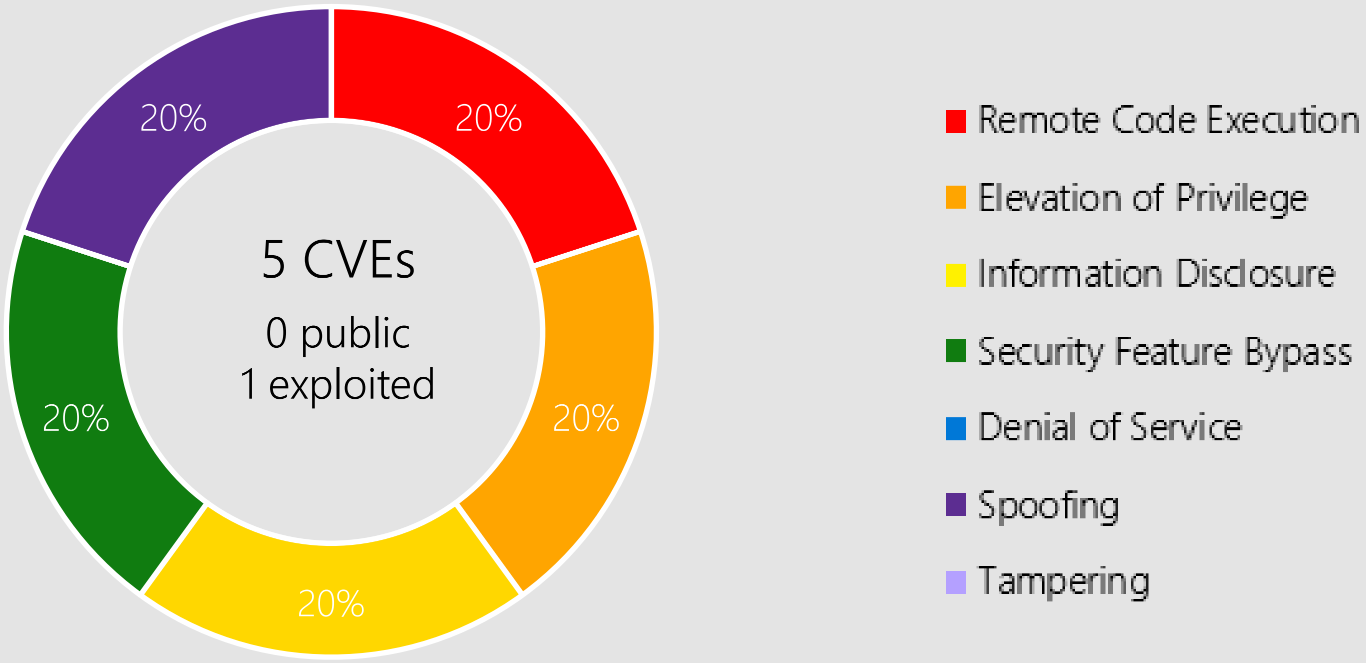
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

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

# Microsoft Office



Microsoft Office-related software

## Products:

Word 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps  Enterprise
Office  Android
Office  Universal
Office 2019  for Mac
Office LTSC  for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
OneNote  Android
SharePoint Foundation 2013
SharePoint Server Subscription Edition
SharePoint Server Subscription Edition Language Pack

# CVE-2023-21715 Publisher

## Impact, Severity, Disclosure

Security Feature Bypass | Important | Privately disclosed | Exploitation Detected

## 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

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

365 Apps Enterprise

# CVE-2023-21716 Word

## 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

Prevent Office from opening RTF documents
**MS08-026: How to prevent Word from loading RTF files**
**Error message in Office when a file is blocked by registry policy settings**

## Affected Software

SharePoint Server 2019
SharePoint Enterprise Server 2013
SharePoint Enterprise Server 2016
Word 2016
Word 2013
SharePoint Foundation 2013
Office Web Apps Server 2013
SharePoint Server Subscription Edition
Office LTSC 2021
Office LTSC for Mac 2021
365 Apps Enterprise
Office 2019 for Mac
Office Online Server
SharePoint Server Subscription Edition Languag Pack

# CVE-2023-21717 SharePoint Server

## Impact, Severity, Disclosure

Elevation of Privilege | 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

# Other Products

## Exchange Server

### CVE-2023-21529 | Important | 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: Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 11.

### CVE-2023-21706 | Important | 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: Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12, Exchange Server 2016 Cumulative Update 23.

# Other Products

## Exchange Server

CVE-2023-21707 | Important | 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: Exchange Server 2019 Cumulative Update 11, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 23, Exchange Server 2019 Cumulative Update 12.

CVE-2023-21710 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: High
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 12, Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 23.

# Other Products

## Dynamics 365

### CVE-2023-21778 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.3
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 Unified Service Desk.

### CVE-2023-21807 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.8
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

# Other Products

## Dynamics 365

### CVE-2023-21570 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

### CVE-2023-21571 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

# Other Products

## Dynamics 365

### CVE-2023-21572 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

### CVE-2023-21573 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 5.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.0, Dynamics 365 (on-premises) version 9.1.

# Other Products

## SQL Server

### CVE-2023-21718 | Critical | 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: SQL Server 2017 (CU 31), SQL Server 2016 Azure Connectivity Pack, SQL Server 2019 (CU 18), SQL Server 2022 (GDR), SQL Server 2016 (GDR), SQL Server 2014 (GDR), SQL Server 2017 (GDR), SQL Server 2019 (GDR), SQL Server 2014 (CU 4).

### CVE-2023-21713 | Important | 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: SQL Server 2019 (CU 18), SQL Server 2017 (GDR), SQL Server 2022 (GDR), SQL Server 2017 (CU 31), SQL Server 2016 (GDR), SQL Server 2014 (CU 4), SQL Server 2016 Azure Connectivity Pack, SQL Server 2019 (GDR), SQL Server 2014 (GDR).

# Other Products

## SQL Server

### CVE-2023-21705 | Important | 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: SQL Server 2017 (CU 31), SQL Server 2016 Azure Connectivity Pack, SQL Server 2019 (CU 18), SQL Server 2022 (GDR), SQL Server 2016 (GDR), SQL Server 2014 (GDR), SQL Server 2017 (GDR), SQL Server 2019 (GDR), SQL Server 2014 (CU 4).

### CVE-2023-21704 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: SQL Server 2019 (CU 18), SQL Server 2016 Azure Connectivity Pack, SQL Server 2022 (GDR), SQL Server 2017 (CU 31), SQL Server 2016 (GDR), SQL Server 2014 (GDR), SQL Server 2017 (GDR), SQL Server 2019 (GDR), SQL Server 2014 (CU 4).

# Other Products

## SQL Server

### CVE-2023-21528 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: SQL Server 2017 (CU 31), SQL Server 2017 (GDR), SQL Server 2022 (GDR), SQL Server 2019 (CU 18), SQL Server 2014 (CU 4), SQL Server 2019 (GDR), SQL Server 2016 Azure Connectivity Pack, SQL Server 2014 (GDR), SQL Server 2016 (GDR).

### CVE-2023-21568 | 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: SQL Server 2022 (GDR), SQL Server 2019 (CU 18), SQL Server 2017 (GDR), SQL Server 2016 (GDR), SQL Server 2016 Azure Connectivity Pack, SQL Server 2017 (CU 31), SQL Server 2014 (CU 4), SQL Server 2019 (GDR), SQL Server 2014 (GDR).

# Other Products

## .NET 6.0 and .NET 7.0

CVE-2023-21808 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.4
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET 7.0, .NET 6.0.

# Other Products

## .NET Framework

CVE-2023-21808 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.4
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.8.1 on Windows 10  20H2, .NET Framework 3.5 AND 4.8.1 on Windows 10  21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 4.8 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Server 2016, .NET Framework 4.8 on Server 2012, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 3.5 AND 4.8.1 on Windows 11  22H2, .NET Framework 3.5 AND 4.8 on Windows 10  1607, .NET Framework 3.5 AND 4.7.2 on Server 2016, .NET Framework 3.5 AND 4.7.2 on Windows 10  1607, .NET Framework 3.5 AND 4.8 on Windows 10  22H2, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 10  22H2, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Windows 10  20H2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 4.8 on Server 2012 R2, .NET Framework 3.5 AND 4.8 on Windows 10  1809, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.7.2 on Server 2019, .NET Framework 3.5 AND 4.8 on Windows 10  21H2, .NET Framework 3.5 AND 4.7.2 on Windows 10  1809

# Other Products

## .NET Framework

CVE-2023-21722 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 4.4
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: Required
Products: .NET Framework 3.5 and 4.6.2 on Windows 10, .NET Framework 4.6.2 on Server 2008, .NET Framework 3.0  on Server 2008, .NET Framework 2.0  on Server 2008, .NET Framework 3.5 AND 4.8.1 on Windows 10  21H2, .NET Framework 3.5 AND 4.8.1 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8.1 on Windows 10  22H2, .NET Framework 3.5 AND 4.8.1 on Windows 11  22H2, .NET Framework 3.5 AND 4.8 on Windows 10  1607, .NET Framework 3.5 AND 4.8 on Windows 10  22H2, .NET Framework 3.5 AND 4.7.2 on Windows 10  1607, .NET Framework 3.5 AND 4.8 on Server 2016, .NET Framework 3.5 on Server 2012 R2, .NET Framework 3.5 on Server 2012, .NET Framework 3.5 AND 4.7.2 on Server 2016, .NET Framework 3.5.1 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Server 2022, .NET Framework 3.5 AND 4.8 on Server 2019, .NET Framework 3.5 AND 4.8 on Windows 11 version 21H2, .NET Framework 3.5 AND 4.8 on Windows 10  20H2, .NET Framework 4.8 on Server 2012, .NET Framework 4.8 on Server 2008 R2, .NET Framework 3.5 AND 4.8 on Windows 10  1809, .NET Framework 4.8 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012 R2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2012, .NET Framework 3.5 AND 4.8.1 on Windows 10  20H2, .NET Framework 3.5 AND 4.8.1 on Server 2022, .NET Framework 3.5 AND 4.7.2 on Windows 10  1809, .NET Framework 3.5 AND 4.8 on Windows 10  21H2, .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Server 2008 R2, .NET Framework 3.5 AND 4.7.2 on Server 2019.

# Other Products

## Visual Studio

CVE-2023-21808 | Critical | Remote Code Execution | Public: No | Exploited: No

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

# Other Products

## Visual Studio

### CVE-2023-21815 | Critical | Remote Code Execution | Public: No | Exploited: No

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

### CVE-2023-23381 | Critical | Remote Code Execution | Public: No | Exploited: No

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

# Other Products

## Visual Studio

### CVE-2023-21566 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2022 version 17.0, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.4, Visual Studio 2022 version 17.2, Visual Studio 2017 version 15.9 (includes 15.0 - 15.8).

### CVE-2023-21567 | Important | Denial of Service | Public: No | Exploited: No

CVSS Base Score 5.6
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2022 version 17.4, Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2022 version 17.2, Visual Studio 2022 version 17.0.

# Other Products

## Azure DevOps Server 2020.1.2

CVE-2023-21553 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Azure DevOps Server 2020.1.2.

# Other Products

## Azure DevOps Server 2022

CVE-2023-21564 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Azure DevOps Server 2022.

# Other Products

## Power BI Report Server - January 2023

CVE-2023-21806 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 8.2
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Power BI Report Server - January 2023.

# Other Products

## Microsoft Defender for Endpoint

CVE-2023-21809 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Microsoft Defender Security Intelligence Updates

# Other Products

## Azure, Store Apps, and Defender for IoT

CVE-2023-23379 Defender for IoT

CVE-2023-21777 Azure App Service on Azure Stack Hub

CVE-2023-21703 Azure Data Box Gateway, Azure Stack Edge

CVE-2023-23382 Azure for Machine Learning

CVE-2023-23377/CVE-2023-23390 3D Builder

CVE-2023-23378 Print 3D

CVE-2019-15126 HoloLens 1

# Product Lifecycle Update

Modern policy February

Microsoft Endpoint Configuration Manager, Version 2107

Major products retiring April 2023

Exchange 2013
Office 2013

aka.ms/lifecycle

Latest Servicing Stack Updates

Microsoft

# Questions?

# Appendix

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21797 | No | No | ODBC Driver |
| CVE-2023-21798 | No | No | ODBC Driver |
| CVE-2023-21800 | No | No | Installer |
| CVE-2023-21802 | No | No | Media |
| CVE-2023-21803 | No | No | iSCSI Discovery Service |
| CVE-2023-21804 | No | No | Graphics Component |
| CVE-2023-21805 | No | No | MSHTML Platform |
| CVE-2023-21811 | No | No | iSCSI Service |
| CVE-2023-21812 | No | No | Common Log File System Driver |
| CVE-2023-21813 | No | No | Secure Channel |
| CVE-2023-21816 | No | No | Active Directory Domain Services API |
| CVE-2023-21817 | No | No | Kerberos |
| CVE-2023-21818 | No | No | Secure Channel |
| CVE-2023-21819 | No | No | Secure Channel |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21820 | No | No | Distributed File System (DFS) |
| CVE-2023-21822 | No | No | Graphics Component |
| CVE-2023-21823 | No | Yes | Graphics Component |
| CVE-2023-21687 | No | No | HTTP.sys |
| CVE-2023-21688 | No | No | NT OS Kernel |
| CVE-2023-21689 | No | No | PEAP |
| CVE-2023-21690 | No | No | PEAP |
| CVE-2023-21691 | No | No | PEAP |
| CVE-2023-21692 | No | No | PEAP |
| CVE-2023-21694 | No | No | Fax Service |
| CVE-2023-21695 | No | No | PEAP |
| CVE-2023-21697 | No | No | Internet Storage Name Service (iSNS) Server |
| CVE-2023-21699 | No | No | Internet Storage Name Service (iSNS) Server |
| CVE-2023-21700 | No | No | iSCSI Discovery Service |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21701 | No | No | Protected Extensible Authentication Protocol (PEAP) |
| CVE-2023-21702 | No | No | iSCSI Service |
| CVE-2023-23376 | No | Yes | Common Log File System Driver |
| CVE-2023-21794 | No | No | Edge (Chromium-based) |
| CVE-2023-21720 | No | No | Edge (Chromium-based) |
| CVE-2023-23374 | No | No | Edge (Chromium-based) |
| CVE-2023-21721 | No | No | OneNote |
| CVE-2023-21714 | No | No | Office |
| CVE-2023-21715 | No | Yes | Office |
| CVE-2023-21716 | No | No | Word |
| CVE-2023-21717 | No | No | SharePoint Server |
| CVE-2023-21528 | No | No | SQL Server |
| CVE-2023-21684 | No | No | PostScript Printer Driver |
| CVE-2023-21777 | No | No | Azure App Service on Azure Stack Hub |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21778 | No | No | Dynamics Unified Service Desk |
| CVE-2023-21806 | No | No | Power BI Report Server |
| CVE-2023-21807 | No | No | Dynamics 365 (on-premises) Cross-site Scripting |
| CVE-2023-21704 | No | No | ODBC Driver for SQL Server |
| CVE-2023-21705 | No | No | SQL Server |
| CVE-2023-21706 | No | No | Exchange Server |
| CVE-2023-21707 | No | No | Exchange Server |
| CVE-2023-21718 | No | No | SQL ODBC Driver |
| CVE-2023-21566 | No | No | Visual Studio |
| CVE-2023-21567 | No | No | Visual Studio |
| CVE-2023-21568 | No | No | SQL Server Integration Service (VS extension) |
| CVE-2023-21570 | No | No | Dynamics 365 (on-premises) Cross-site |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21573 | No | No | Dynamics 365 (on-premises) Cross-site Scripting |
| CVE-2023-23378 | No | No | Print 3D |
| CVE-2023-23379 | No | No | Defender for IoT |
| CVE-2023-23382 | No | No | Azure Machine Learning Compute Instance |
| CVE-2023-21529 | No | No | Exchange Server |
| CVE-2023-21553 | No | No | Azure DevOps Server |
| CVE-2023-21799 | No | No | WDAC OLE DB provider for SQL Server |
| CVE-2023-21801 | No | No | PostScript Printer Driver |
| CVE-2023-21808 | No | No | .NET and Visual Studio |
| CVE-2023-21809 | No | No | Defender for Endpoint |
| CVE-2023-21815 | No | No | Visual Studio |
| CVE-2023-21685 | No | No | WDAC OLE DB provider for SQL Server |
| CVE-2023-21686 | No | No | WDAC OLE DB provider |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2023-21703 | No | No | Azure Data Box Gateway |
| CVE-2023-21710 | No | No | Exchange Server |
| CVE-2023-21713 | No | No | SQL Server |
| CVE-2023-21722 | No | No | .NET |
| CVE-2023-21564 | No | No | Azure DevOps Server Cross-Site Scripting |
| CVE-2023-23377 | No | No | 3D Builder |
| CVE-2023-23381 | No | No | Visual Studio Code |
| CVE-2023-23390 | No | No | 3D Builder |
| CVE-2019-15126 | No | No | MITRE: CVE-2019-15126 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |