Microsoft

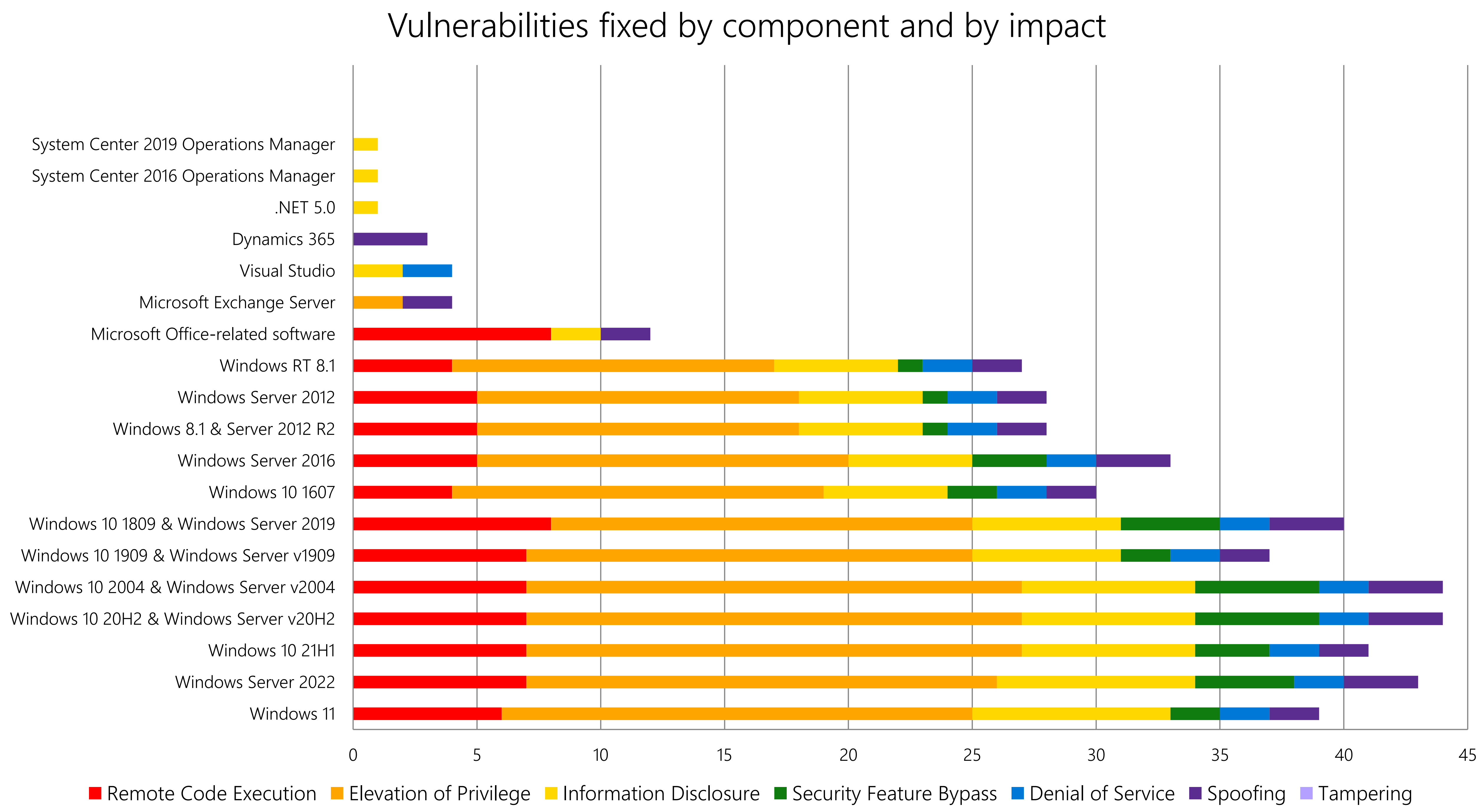
# Microsoft Security Release

October 12, 2021

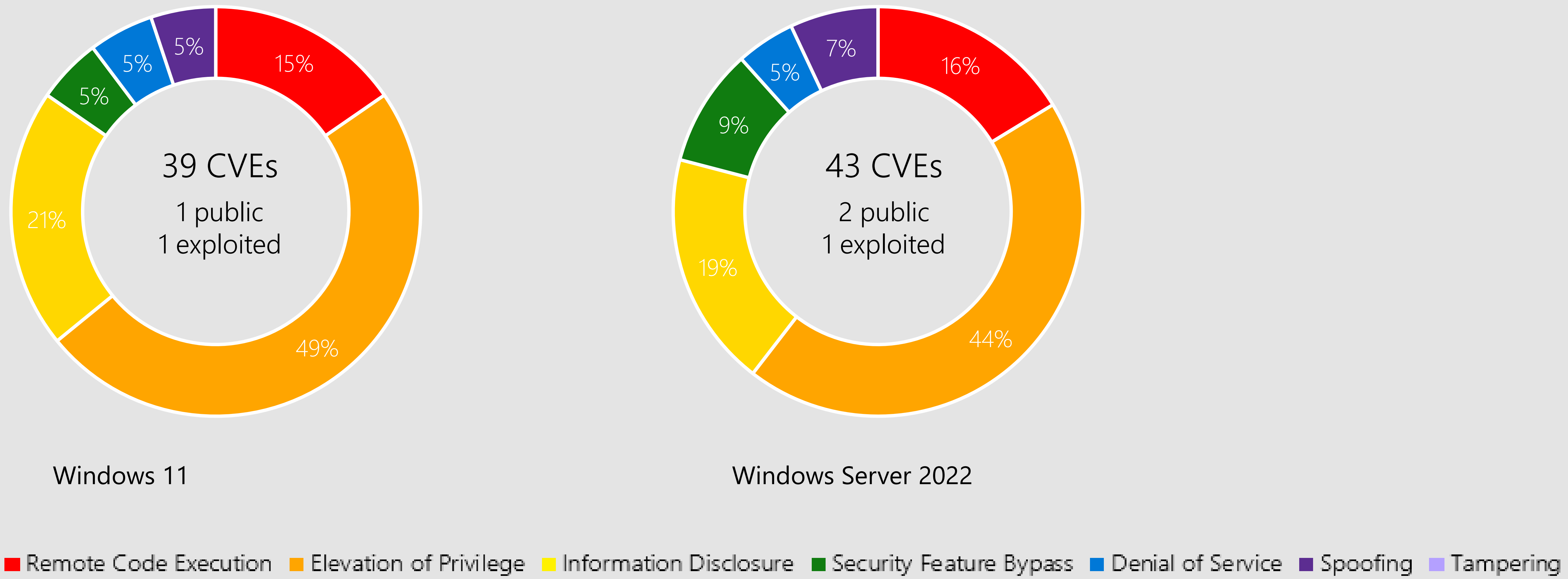
# Agenda

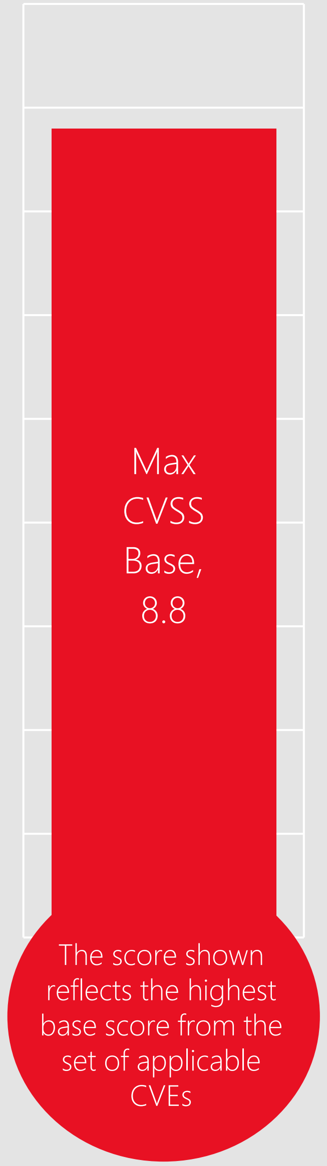
- Security Updates
- Product Support Lifecyle
- Other resources related to the release

# Monthly Security Release Overview - October 2021



# Windows 11, Server 2022





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

## Affected Components:

- Active Directory
- ADFS
- Hyper-V
- Installer
- Kernel
- AppContainer Elevation Of Privilege
- AppContainer Firewall Rules
- AppX Deployment Service
- Print Spooler
- Bind Filter Driver
- Cloud Files Mini Filter Driver
- CLFS Driver
- MSHTML Platform
- NAT
- Desktop Bridge
- DirectX Graphics Kernel
- DNS Server
- Nearby Sharing
- Rich Text Edit Control
- DWM Core Library
- Event Tracing
- exFAT File System
- RPC Runtime
- Storage Spaces Controller
- Fast FAT File System Driver
- Graphics Component
- HTTP.sys
- TCP/IP
- Media Foundation Dolby Digital Atmos Decoders

# CVE-2021-36970 Print Spooler

## Impact, Severity, Disclosure

Spoofing | 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

Server, version 20H2
Server, version 2004
Server 2019
Windows 10
Windows 11
Server 2016
Server 2012 R2
Server 2012
Windows 8.1
Server 2022

# CVE-2021-40449 Win32k

## 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.

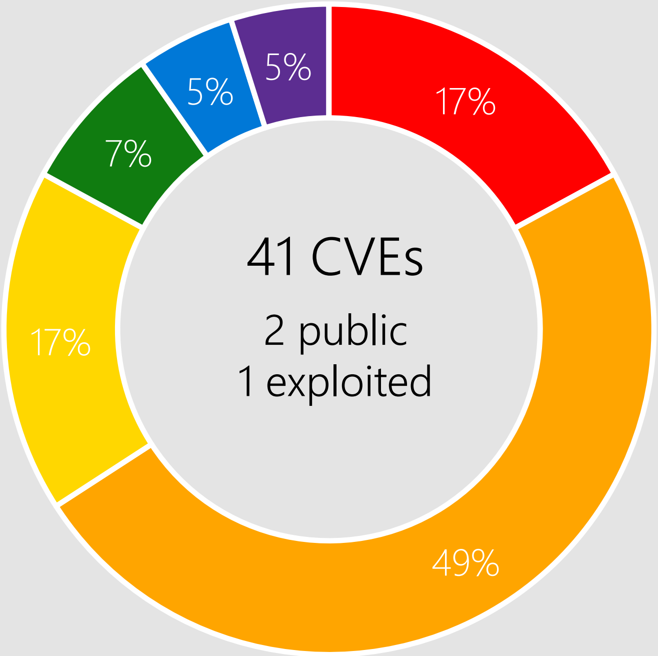
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

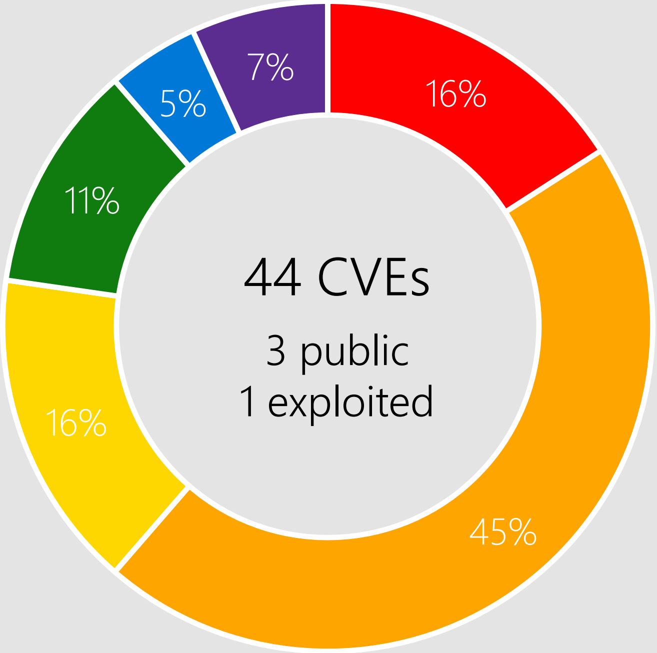
## Affected Software

Windows 11
Server 2022
Server, version 20H2
Server, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

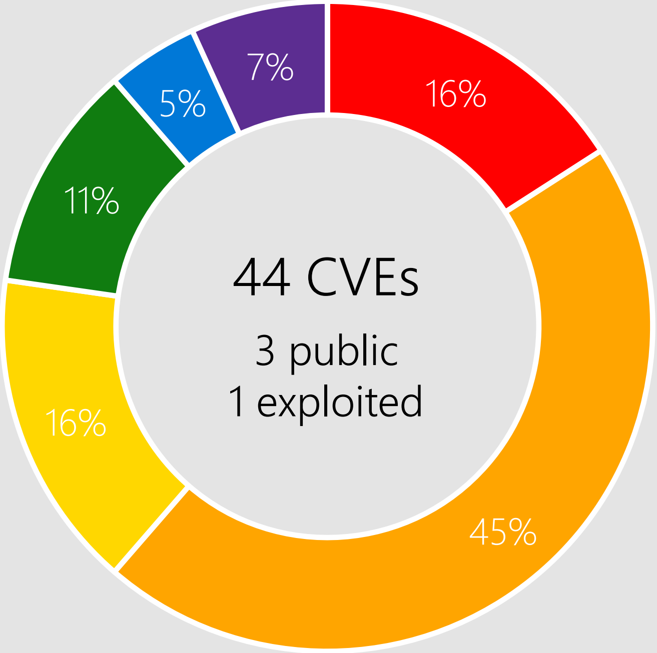
# Windows 10



Windows 10 21H1

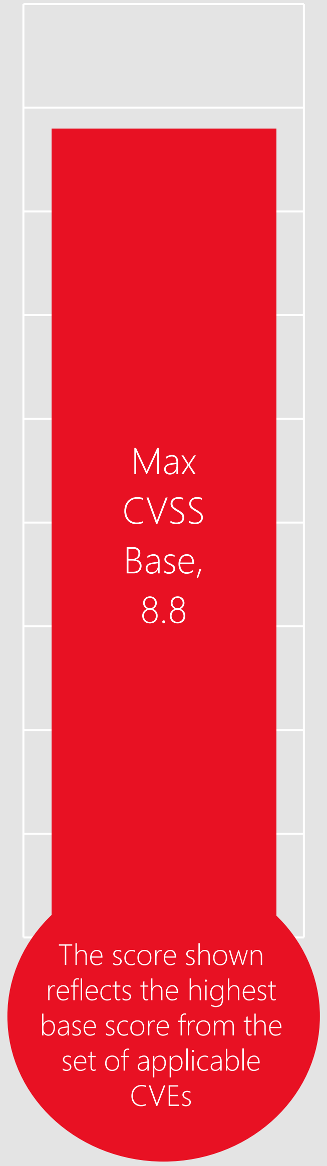


Windows 10 20H2 & Windows Server v20H2



Windows 10 2004 & Windows Server v2004

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



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

## Affected Components:

Active Directory
ADFS
HTTP.sys
Hyper-V
Installer
Text Shaping

AppContainer Elevation Of Privilege
AppContainer Firewall Rules
AppX Deployment Service
Storage Spaces Controller

Bind Filter Driver
Cloud Files Mini Filter Driver
CLFS Driver
NAT
Nearby Sharing

Console Window Host
Desktop Bridge
DirectX Graphics Kernel
Kernel
Media Audio Decoder
Media Foundation

DNS Server
DWM Core Library
Event Tracing
Print Spooler
RPC Runtime
TCP/IP

exFAT File System
Fast FAT File System Driver
Graphics Component
Rich Text Edit Control
Media Foundation Dolby Digital Atmos Decoders

# CVE-2021-40469 DNS Server

## Impact, Severity, Disclosure

Remote Code Execution | Important | Publicly Disclosed | No known exploits in the wild

## CVSSScoreMetrics

Base CVSS Score: 7.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | User Interaction: None

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

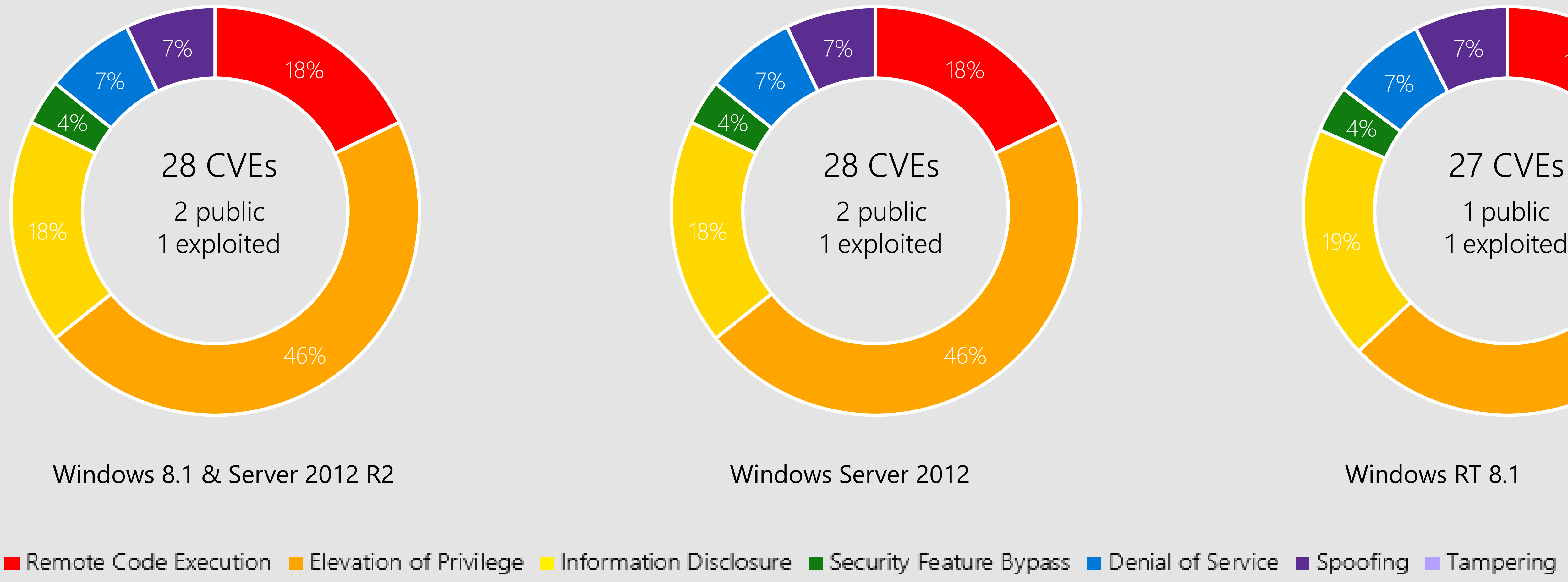
## Workarounds

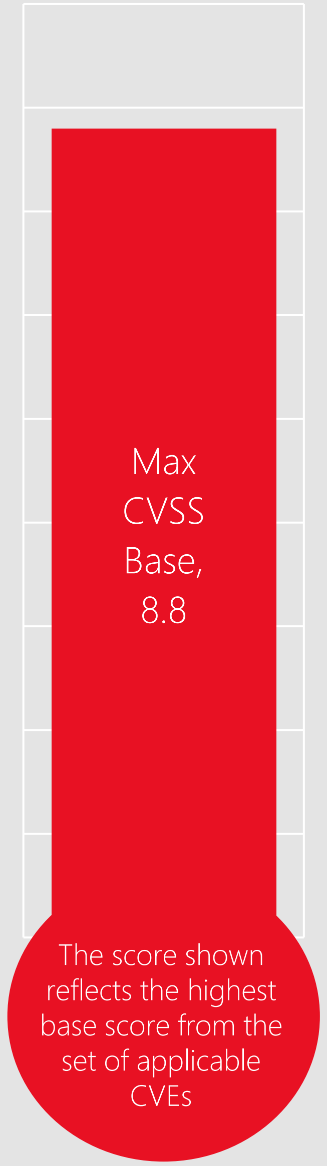
Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

Server 2022
Server, version 20H2
Server, version 2004
Server 2019
Server 2016
Server 2012 R2
Server 2012

# Windows 8.1, Server 2012 R2, and Server 2012




Max CVSS Base, 8.8

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

## Affected Components:

- AppContainer Elevation Of Privilege
- Common Log File System Driver
- DNS Server
- Event Tracing
- exFAT File System
- Fast FAT File System Driver
- Graphics Component
- HTTP.sys
- Installer
- Kernel
- Media Audio Decoder
- MSHTML Platform
- NAT
- Print Spooler
- Remote Procedure Call Runtime
- Rich Text Edit Control
- Storage Spaces Controller
- TCP/IP

# CVE-2021-40461 Hyper-V

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

Base CVSS Score: 8 | Attack Vector: Adjacent | 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
Server 2022
Server, version 20H2
Windows 10
Server, version 2004
Server 2019

# CVE-2021-41340 Graphics Component

## 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.

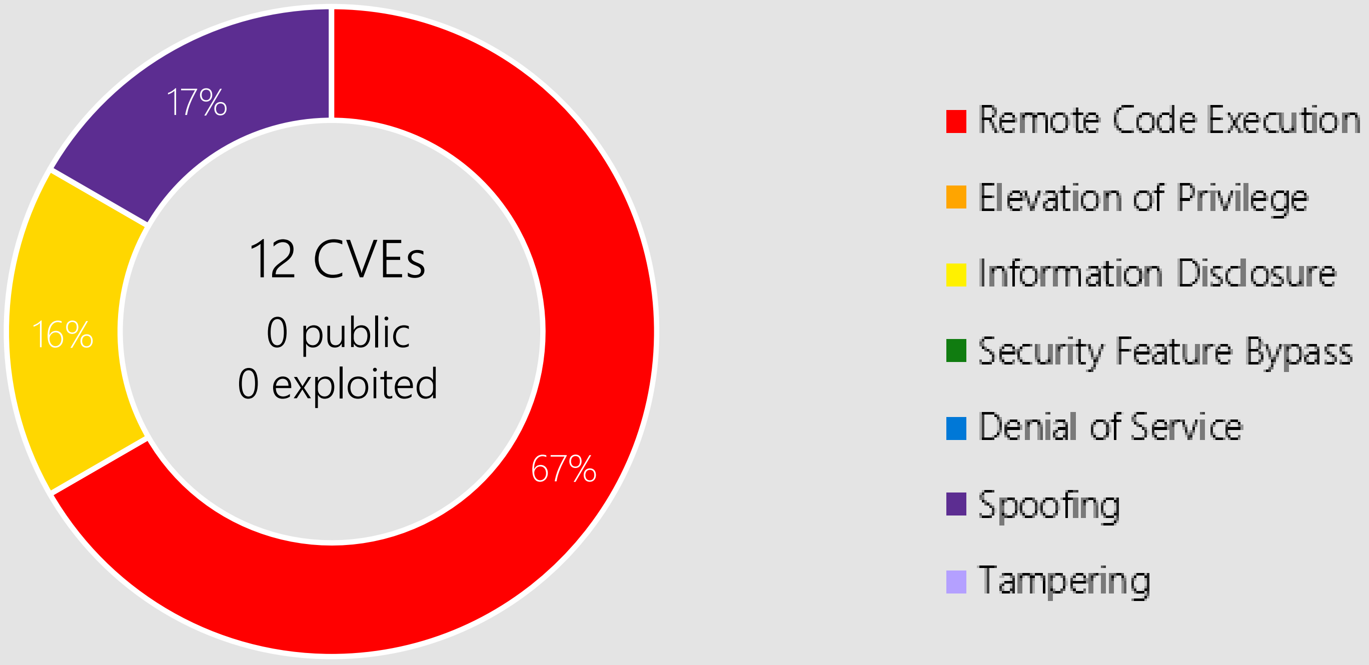
## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

Windows 11
Server 2022
Server, version 20H2
Server, version 2004
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
Word 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office LTSC for Mac 2021
Office LTSC 2021
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013

# CVE-2021-40487 SharePoint Server

## 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 Foundation 2013
SharePoint Server 2019
SharePoint Enterprise Server 2016

# CVE-2021-40486 Word

## 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: 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

Word 2016
Office Online Server
Word 2013
Office Web Apps Server 2013
SharePoint Enterprise Server 2013
SharePoint Enterprise Server 2016
Office 2019
SharePoint Server 2019

# CVE-2021-40485 Excel

## Impact, Severity, Disclosure

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

## CVSSScoreMetrics

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

## Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

## Workarounds

Microsoft has not identified any workarounds for this vulnerability.

## Affected Software

Office LTSC 2021
Office LTSC for Mac 2021
Excel 2013
Excel 2016
365 Apps Enterprise
Office 2019
SharePoint Enterprise Server 2013
Office Online Server
Office 2019 for Mac

# CVE-2021-40480 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

# Other Products

## Exchange Server

### CVE-2021-26427 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 9
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11.

### CVE-2021-41348 | Important | Elevation of Privilege | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10.

# Other Products

## Exchange Server

CVE-2021-34453 | 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: Exchange Server 2016 Cumulative Update 21, Exchange Server 2016 Cumulative Update 22, Exchange Server 2019 Cumulative Update 11, Exchange Server 2019 Cumulative Update 10.

CVE-2021-41350 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2019 Cumulative Update 11, Exchange Server 2016 Cumulative Update 22, Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10.

# Other Products

## Dynamics 365

### CVE-2021-40457 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 7.4
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Dynamics 365 Customer Engagement V9.0, Dynamics 365 Customer Engagement V9.1.

### CVE-2021-41353 | 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 9.1, Dynamics 365 (on-premises) version 9.0.

# Other Products

## Dynamics 365

CVE-2021-41354 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 4.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 (on-premises) version 9.1, Dynamics 365 (on-premises) version 9.0.

# Other Products

## System Center 2016/2019 Operations Manager

CVE-2021-41352 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: System Center 2016 Operations Manager, System Center 2019 Operations Manager, System Center 2012 R2 Operations Manager

# Other Products

## .NET 5.0

CVE-2021-41355 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.7
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0.

# Other Products

## Visual Studio

### CVE-2021-41355 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 5.7
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0.

# Other Products

## Visual Studio

### CVE-2020-1971 | Important | Denial of Service | Public: No | Exploited: No

Products: Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3).

### CVE-2021-3449 | Important | Denial of Service | Public: No | Exploited: No

Products: Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3).

### CVE-2021-3450 | Important | Information Disclosure | Public: No | Exploited: No

Products: Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.11 (includes 16.0 - 16.10), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2017 version 15.9 (includes 15.0 - 15.8), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3).

# Other Products

## Intune management extension

CVE-2021-41363 | Important | Security Feature Bypass | Public: No | Exploited: No

CVSS Base Score 4.2
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: None
Products: Intune management extension.

# Product Lifecycle Update

Fixed lifecycle products reaching end of support in October

Silverlight 5
Visual Studio 2019, ver. 16.4

Modern lifecycle products reaching end of servicing in October

Endpoint Config Manager, ver. 2002
Dynamics 365 Business Central on-premises, 2020 release wave 1, version 16.x

aka.ms/lifecycle

Microsoft

# Questions?

# Appendix

# Printing Guidance

Restricting installation of new printer drivers after applying the July 6, 2021 updates: KB5005010

Manage new Point and Print default driver installation behavior: KB5005652

Managing deployment of Printer RPC binding changes for CVE-2021-1678: KB4599464

Monitor Windows release health for issues being addressed https://docs.microsoft.com/en-us/windows/release-health/

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-36953 | No | No | TCP/IP |
| CVE-2021-36970 | No | No | Print Spooler |
| CVE-2021-40443 | No | No | Common Log File System Driver |
| CVE-2021-40449 | No | Yes | Win32k |
| CVE-2021-40455 | No | No | Installer |
| CVE-2021-40456 | No | No | AD FS |
| CVE-2021-40475 | No | No | Cloud Files Mini Filter Driver |
| CVE-2021-40476 | No | No | AppContainer Elevation Of Privilege |
| CVE-2021-40477 | No | No | Event Tracing |
| CVE-2021-40478 | No | No | Storage Spaces Controller |
| CVE-2021-38662 | No | No | Fast FAT File System Driver |
| CVE-2021-38663 | No | No | exFAT File System |
| CVE-2021-38672 | No | No | Hyper-V |
| CVE-2021-40450 | No | No | Win32k |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-40460 | No | No | RPC Runtime |
| CVE-2021-40461 | No | No | Hyper-V |
| CVE-2021-40462 | No | No | Media Foundation Dolby Digital Atmos Decoders |
| CVE-2021-40463 | No | No | NAT |
| CVE-2021-40464 | No | No | Nearby Sharing |
| CVE-2021-40465 | No | No | Text Shaping |
| CVE-2021-40466 | No | No | Common Log File System Driver |
| CVE-2021-40467 | No | No | Common Log File System Driver |
| CVE-2021-40468 | No | No | Bind Filter Driver |
| CVE-2021-40469 | Yes | No | DNS Server |
| CVE-2021-40470 | No | No | DirectX Graphics Kernel |
| CVE-2021-40488 | No | No | Storage Spaces Controller |
| CVE-2021-40489 | No | No | Storage Spaces Controller |
| CVE-2021-26441 | No | No | Storage Spaces Controller |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-26442 | No | No | HTTP.sys |
| CVE-2021-41330 | No | No | Media Foundation |
| CVE-2021-41331 | No | No | Media Audio Decoder |
| CVE-2021-41332 | No | No | Print Spooler |
| CVE-2021-41334 | No | No | Desktop Bridge |
| CVE-2021-41335 | Yes | No | Kernel |
| CVE-2021-41336 | No | No | Kernel |
| CVE-2021-41337 | No | No | Active Directory |
| CVE-2021-41338 | Yes | No | AppContainer Firewall Rules |
| CVE-2021-41340 | No | No | Graphics Component |
| CVE-2021-41342 | No | No | MSHTML Platform |
| CVE-2021-41343 | No | No | Fast FAT File System Driver |
| CVE-2021-41345 | No | No | Storage Spaces Controller |
| CVE-2021-41347 | No | No | AppX Deployment Service |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-41357 | No | No | Win32k |
| CVE-2021-37974 | No | No | Chromium |
| CVE-2021-37975 | No | No | Chromium |
| CVE-2021-37976 | No | No | Chromium |
| CVE-2021-41344 | No | No | SharePoint Server |
| CVE-2021-40471 | No | No | Excel |
| CVE-2021-40472 | No | No | Excel |
| CVE-2021-40473 | No | No | Excel |
| CVE-2021-40474 | No | No | Excel |
| CVE-2021-40479 | No | No | Excel |
| CVE-2021-40480 | No | No | Office Visio |
| CVE-2021-40481 | No | No | Office Visio |
| CVE-2021-40482 | No | No | SharePoint Server |
| CVE-2021-40483 | No | No | SharePoint Server |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-40484 | No | No | SharePoint Server |
| CVE-2021-40485 | No | No | Excel |
| CVE-2021-40486 | No | No | Word |
| CVE-2021-40487 | No | No | SharePoint Server |
| CVE-2021-34453 | No | No | Exchange Server |
| CVE-2021-40454 | No | No | Rich Text Edit Control |
| CVE-2021-40457 | No | No | Dynamics 365 Customer Engagement |
| CVE-2021-41348 | No | No | Exchange Server |
| CVE-2021-41350 | No | No | Exchange Server |
| CVE-2021-41355 | No | No | .NET Core and Visual Studio |
| CVE-2021-41361 | No | No | Active Directory Federation Server |
| CVE-2021-3450 | No | No | OpenSSL |
| CVE-2021-3449 | No | No | OpenSSL |
| CVE-2020-1971 | No | No | OpenSSL |

| CVE | Public | Exploited | Product |
|---|---|---|---|
| CVE-2021-26427 | No | No | Exchange Server |
| CVE-2021-41339 | No | No | DWM Core Library |
| CVE-2021-41346 | No | No | Console Window Host |
| CVE-2021-41352 | No | No | SCOM |
| CVE-2021-41353 | No | No | Dynamics 365 Sales |
| CVE-2021-41354 | No | No | Dynamics 365 (on-premises) Cross-site Scripting |
| CVE-2021-41363 | No | No | Intune Management Extension |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |