Microsoft

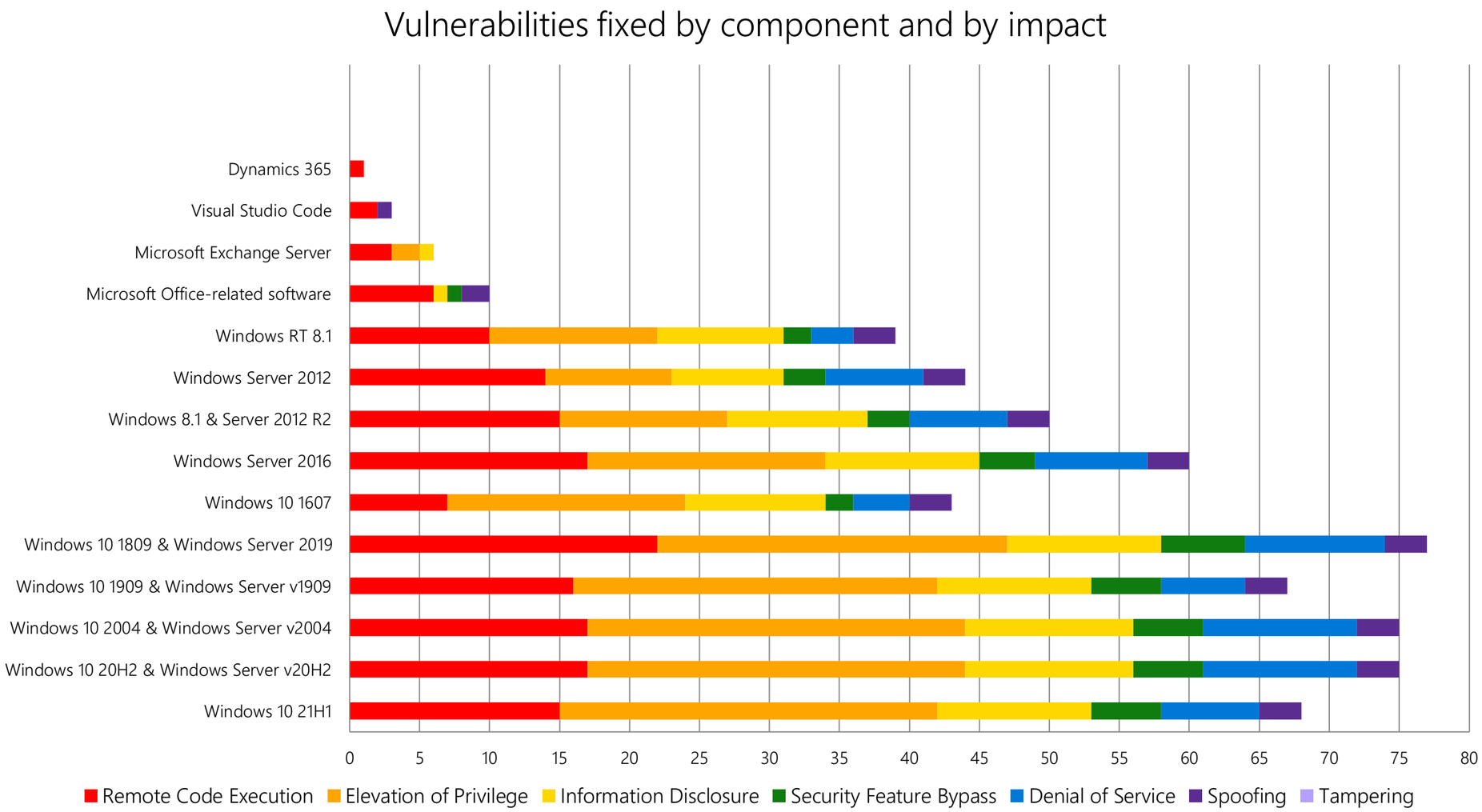
Microsoft Security Release

July 13, 2021

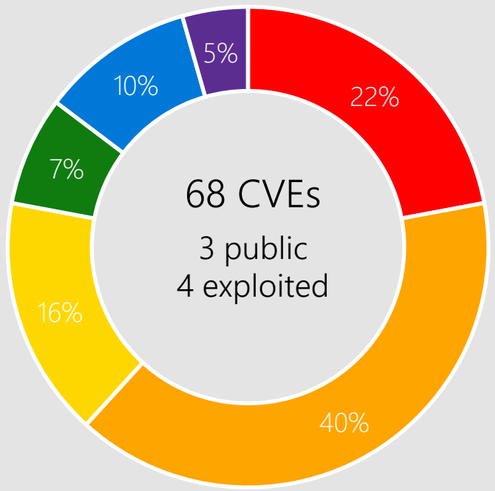
Agenda

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

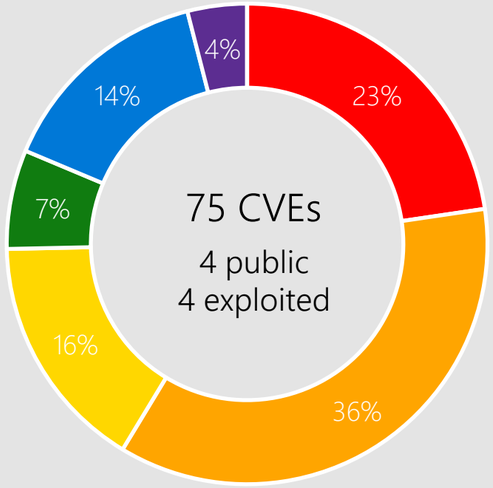
Monthly Security Release Overview - July 2021



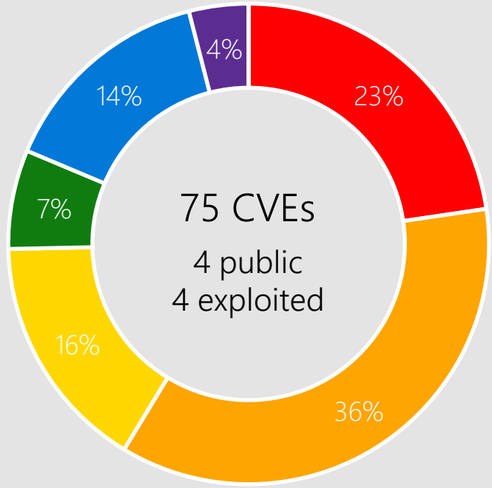
Windows 10



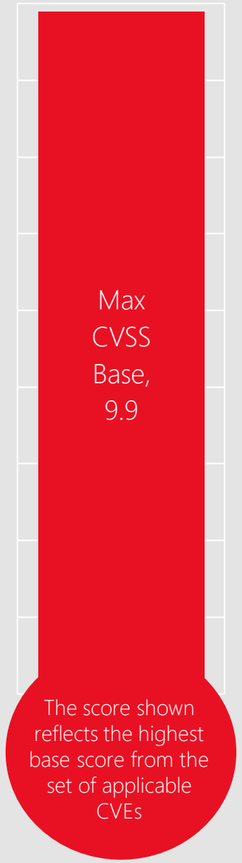
Windows 10 21H1



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

Affected Components:

Active Directory
Address Book
AF_UNIX Socket Provider
AppContainer
AppX Deployment Extensions
Authenticode
Bowser.sys
Certificate
Cloud Files Mini Filter- Driver
Console Driver
Desktop Bridge
DirectWrite
DNS Server
DNS Snap-in
Event Tracing
File History Service
Font Driver Host
GD/ GDI+
HTML Platform
Hyper-V
Installer
InstallService
Kernel
Kernel Memory
Key Distribution Center
LSA
Media
Media Foundation
MSHTML Platform
Partition Management Driver
Print Spooler
Projected File System
Remote Access Connection Manager
Remote Assistance
Scripting Engine
Secure Kernel Mode
Security Account Manager-Remote Protocol
SMB
Storage Spaces Controller
TCP/IP Driver
Win32k

CVE-2021-34458 Kernel

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 9.9 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

More Information

This issue allows a single root input/output virtualization (SR-IOV) device which is assigned to a guest to potentially interfere with its Peripheral Component Interface Express (PCIe) siblings which are attached to other guests or to the root.

You will be vulnerable if you implement the following:

Your Windows instance is hosting virtual machines
Your Server includes the required hardware with SR-IOV devices.

Affected Software

Server, version 20H2
Server, version 2004
Server 2019
Server 2016

CVE-2021-31979/33771 Kernel

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

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

CVE-2021-34450 Hyper-V

Impact, Severity, Disclosure

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

CVSSScoreMetrics

Base CVSS Score: 8.5 | Attack Vector: Network | Attack Complexity: High | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

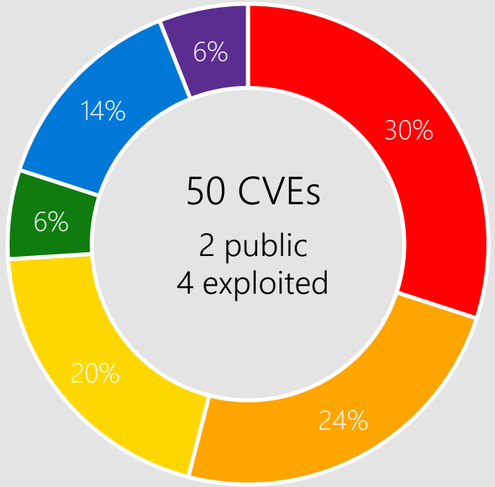
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

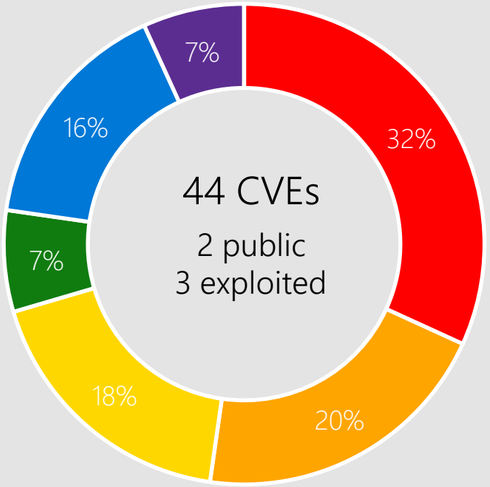
Affected Software

Server, version 20H2
Windows 10
Server, version 2004
Server 2019

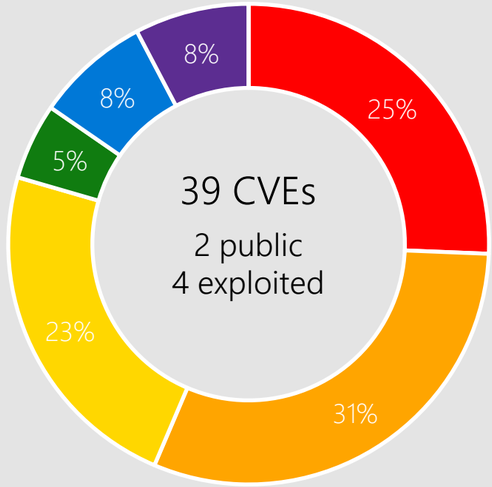
Windows 8.1, Server 2012 R2, and Server 2012



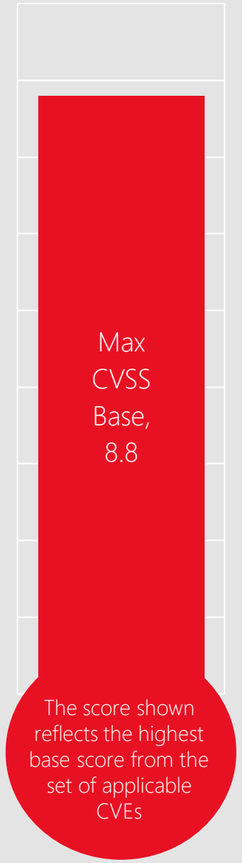
Windows 8.1 & Server 2012 R2



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:

Address Book
AppContainer
Authenticode
Bowser.sys
Certificate
DNS Server
DNS Snap-in
File History Service
GDI/ GDI+
HTML Platform
Installer
Kernel
Kernel Memory
Key Distribution Center
LSA
Media Foundation
MSHTML Platform
Print Spooler
Remote Access Connection Manager
Remote Assistance
Scripting Engine
Security Account Manager
Remote Protocol
SMB
Storage Spaces Controller
TCP/IP Driver
Win32k

CVE-2021-34494 DNS Server

Impact, Severity, Disclosure

Remote Code Execution | Critical | 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: 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, version 20H2
Server, version 2004
Server 2019
Server 2016
Server 2012 R2
Server 2012

CVE-2021-34527 Print Spooler (released OOB)

Impact, Severity, Disclosure

Remote Code Execution | Critical | Publicly Disclosed | Exploitation Detected

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

Option 1: disable the Print Spooler service.
Option 2: disable inbound remote printing through GPO
See Security Update Guide for details.

Affected Software

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

CVE-2021-34448 Scripting Engine

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | Exploitation Detected

CVSSScoreMetrics

Base CVSS Score: 6.8 | Attack Vector: Network | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

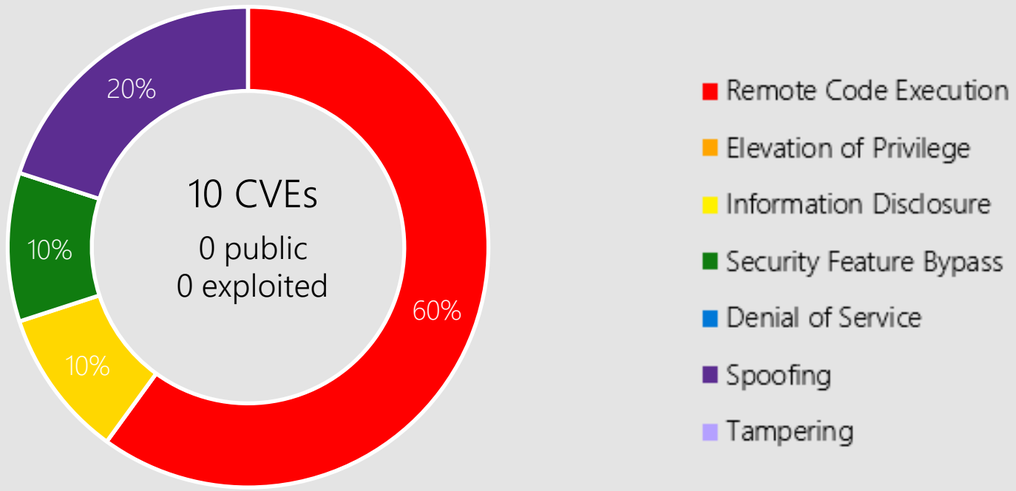
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server 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 2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2013/2016
365 Apps Enterprise
Office 2019 for Mac
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013

CVE-2021-34501 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

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

CVE-2021-34452 Word

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

Word 2016
365 Apps Enterprise
Office 2019

CVE-2021-34520 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

Other Products

Exchange Server

CVE-2021-33768 | 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 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20.

CVE-2021-34470 | 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 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23. Applying the CU addresses the CVE. There is no separate security update for this CVE.

Other Products

Exchange Server

CVE-2021-31196 | 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 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20.

CVE-2021-31206 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.6
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2016 Cumulative Update 21, Exchange Server 2019 Cumulative Update 10, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20.

Other Products

Exchange Server

CVE-2021-34473 | Critical | Remote Code Execution | Public: Yes | Exploited: No

CVSS Base Score 9.1
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2016 Cumulative Update 20, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9. This CVE was documented in July, but was included in the April 2021 release.

CVE-2021-34523 | Important | Elevation of Privilege | Public: Yes | Exploited: No

CVSS Base Score 9
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2016 Cumulative Update 20, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9. This CVE was documented in July, but was included in the April 2021 release.

Other Products

Exchange Server

CVE-2021-33766 | Important | Information Disclosure | Public: No | Exploited: No

CVSS Base Score 7.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20. This CVE was documented in July, but was included in the April 2021 release.

More Information about Exchange servicing:
Released: July 2021 Exchange Server Security Updates - Microsoft Tech Community

Other Products

Dynamics 365

CVE-2021-34474 | Critical | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
User Interaction: None
Products: Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.3, Dynamics 365 Business Central 2020 Release Wave 2 - Update 17.8, Dynamics 365 Business Central 2020 Release Wave 1 - Update 16.14.

Other Products

Microsoft Malware Protection Engine

CVE-2021-34464 | 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: Malware Protection Engine.

CVE-2021-34522 | 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: Malware Protection Engine.

Other Products

Developer Tools, Power BI, Mobile

CVE-2021-34479/CVE-2021-34528/CVE-2021-34529 Visual Studio Code

CVE-2021-31984 Power BI

CVE-2021-33767 Open Enclave SDK

CVE-2021-33753 Microsoft Bing Search for Android

CVE-2021-34477 .NET Education Bundle SDK Install Tool, .NET Install Tool for Extension Authors

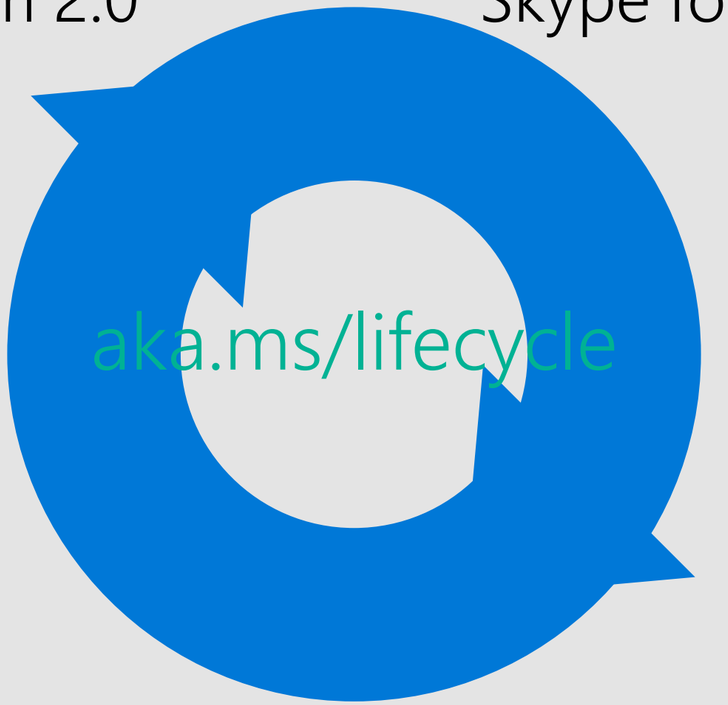
Product Lifecycle Update

Fixed lifecycle products reaching end of support

Dynamics Retail Mgmt. System 2.0
Dynamics CRM 2011
Dynamics SL 2011
SQL Server Compact 4.0

Modern lifecycle products reaching end of support

Skype for Business Online



Helping customers shift to a modern desktop

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5001403	April 2021
Windows Server 2012	5001401	April 2021
Windows 10 1607/Server 2016	5001402	April 2021
Windows 10 1809/Server 2019	5003711	June 2021
Windows 10 1909/Windows Server, version 1909	5004748	July 2021
Windows 10 2004/Windows Server, version 2004	Inc in monthly update	N/A
Windows 10 20H2/Windows Server, version 20H2	Inc in monthly update	N/A

Simplifying on-premises deployment of servicing stack updates - Microsoft Tech Community

Deploy Windows SSUs and LCUs together with one cumulative update - Microsoft Tech Community

Microsoft

Questions?

Appendix

Reminder: Adobe Flash Player End of Support

- On Sep. 4th, Microsoft has published the detailed plan for Adobe Flash Player End of Support.
  - In July 2017, Microsoft, along with Adobe and their industry technology partners, announced that Adobe Flash Player will no longer be supported after December 2020.
  - In keeping with this plan, Microsoft is ending support for Adobe Flash Player on Microsoft Edge (both the new Microsoft Edge and Microsoft Edge Legacy) and Internet Explorer 11 at the end of 2020.
  - Edge (Chromium based): Flash has been removed at Version 88 (January 2021)
  - Microsoft Edge Legacy and Internet Explorer 11
    - January 2021, Adobe Flash Player has been disabled by default and all versions older than KB4561600 released in June 2020 will be blocked.
    - January 2021, Downloadable resources related to Adobe Flash Player that are hosted on Microsoft websites are no longer available.
    - An update titled "Update for Removal of Adobe Flash Player" will be made available via Microsoft Update Catalog, Windows Update and WSUS that permanently removes Adobe Flash Player as a component of the Windows OS devices.
      - If you wish to remove Adobe Flash Player from your systems ahead of the end of support, the update is available for download on the Microsoft Update Catalog
      - The update will be made optional on Windows Update and WSUS and will be made recommended a few months later. It should be noted that this update will be permanent and cannot be un-installed.
        - Updated April 2021 : Starting in June 2021, the KB4577586 "Update for Removal of Adobe Flash Player" will be included in the Preview Update for Windows 10, version 1809 and above platforms. It will also be included in every subsequent Latest Cumulative Update.
        - As of July 2021, the KB4577586 "Update for Removal of Adobe Flash Player" has been included in the Latest Cumulative Update for Windows 10, versions 1607 and Windows 10, version 1507. The KB will also be included in the Monthly Rollup and the Security Only Update for Windows 8.1, Windows Server 2012, and Windows Embedded 8 Standard.
        - Preview of June 2021 included the package that removes Flash July OOB also includes package that removes Flash.
  - In Summer of 2021, all the APIs, group polices and user interfaces that specifically govern the behavior of Adobe Flash Player will be removed

CVE	Public	Exploited	Product
CVE-2021-31183	No	No	TCP/IP Driver
CVE-2021-31947	No	No	HEVC Video Extensions
CVE-2021-31961	No	No	InstallService
CVE-2021-33740	No	No	Media
CVE-2021-33743	No	No	Projected File System
CVE-2021-33744	No	No	Secure Kernel Mode
CVE-2021-33755	No	No	Hyper-V
CVE-2021-33757	No	No	Security Account Manager Remote Protocol
CVE-2021-33758	No	No	Hyper-V
CVE-2021-33759	No	No	Desktop Bridge
CVE-2021-33760	No	No	Media Foundation
CVE-2021-33761	No	No	Remote Access Connection Manager
CVE-2021-33763	No	No	Remote Access Connection Manager
CVE-2021-33765	No	No	Installer

CVE	Public	Exploited	Product
CVE-2021-33771	No	No	Kernel
CVE-2021-33773	No	No	Remote Access Connection Manager
CVE-2021-33774	No	No	Event Tracing
CVE-2021-33780	No	No	DNS Server
CVE-2021-34441	No	No	Media Foundation
CVE-2021-34442	No	No	DNS Server
CVE-2021-34491	No	No	Win32k
CVE-2021-34492	Yes	No	Certificate
CVE-2021-34493	No	No	Partition Management Driver
CVE-2021-34444	No	No	DNS Server
CVE-2021-34494	No	No	DNS Server
CVE-2021-34445	No	No	Remote Access Connection Manager
CVE-2021-34446	No	No	HTML Platform
CVE-2021-34496	No	No	GDI

CVE	Public	Exploited	Product
CVE-2021-34447	No	No	MSHTML Platform
CVE-2021-34497	No	No	MSHTML Platform
CVE-2021-34498	No	No	GDI
CVE-2021-34449	No	No	Win32k
CVE-2021-34499	No	No	DNS Server
CVE-2021-34450	No	No	Hyper-V
CVE-2021-34500	No	No	Kernel Memory
CVE-2021-34521	No	No	Raw Image Extension
CVE-2021-31979	No	No	Kernel
CVE-2021-33745	No	No	DNS Server
CVE-2021-33746	No	No	DNS Server
CVE-2021-33749	No	No	DNS Snap-in
CVE-2021-33750	No	No	DNS Snap-in
CVE-2021-33751	No	No	Storage Spaces Controller

CVE	Public	Exploited	Product
CVE-2021-33752	No	No	DNS Snap-in
CVE-2021-33754	No	No	DNS Server
CVE-2021-33756	No	No	DNS Snap-in
CVE-2021-33764	No	No	Key Distribution Center
CVE-2021-33772	No	No	TCP/IP Driver
CVE-2021-33775	No	No	HEVC Video Extensions
CVE-2021-33776	No	No	HEVC Video Extensions
CVE-2021-33777	No	No	HEVC Video Extensions
CVE-2021-33778	No	No	HEVC Video Extensions
CVE-2021-33779	Yes	No	Active Directory
CVE-2021-33781	Yes	No	Active Directory
CVE-2021-33782	No	No	Authenticode
CVE-2021-33783	No	No	SMB
CVE-2021-33784	No	No	Cloud Files Mini Filter Driver

CVE	Public	Exploited	Product
CVE-2021-33785	No	No	AF_UNIX Socket Provider
CVE-2021-33786	No	No	LSA
CVE-2021-33788	No	No	LSA
CVE-2021-34438	No	No	Font Driver Host
CVE-2021-34439	No	No	Media Foundation
CVE-2021-34488	No	No	Console Driver
CVE-2021-34489	No	No	DirectWrite
CVE-2021-34440	No	No	GDI+
CVE-2021-34490	No	No	TCP/IP Driver
CVE-2021-34503	No	No	Media Foundation
CVE-2021-34454	No	No	Remote Access Connection Manager
CVE-2021-34504	No	No	Address Book
CVE-2021-34455	No	No	File History Service
CVE-2021-34456	No	No	Remote Access Connection Manager

CVE	Public	Exploited	Product
CVE-2021-34457	No	No	Remote Access Connection Manager
CVE-2021-34507	No	No	Remote Assistance
CVE-2021-34458	No	No	Kernel
CVE-2021-34508	No	No	Kernel
CVE-2021-34459	No	No	AppContainer Elevation Of Privilege
CVE-2021-34509	No	No	Storage Spaces Controller
CVE-2021-34460	No	No	Storage Spaces Controller
CVE-2021-34510	No	No	Storage Spaces Controller
CVE-2021-34511	No	No	Installer
CVE-2021-34461	No	No	Container Isolation FS Filter Driver
CVE-2021-34512	No	No	Storage Spaces Controller
CVE-2021-34462	No	No	AppX Deployment Extensions
CVE-2021-34513	No	No	Storage Spaces Controller
CVE-2021-34514	No	No	Kernel

CVE	Public	Exploited	Product
CVE-2021-34464	No	No	Defender
CVE-2021-34516	No	No	Win32k
CVE-2021-34466	No	No	Hello
CVE-2021-34522	No	No	Defender
CVE-2021-34525	No	No	DNS Server
CVE-2021-34527	Yes	Yes	Print Spooler
CVE-2021-34501	No	No	Excel
CVE-2021-34452	No	No	Word
CVE-2021-34467	No	No	SharePoint Server
CVE-2021-34518	No	No	Excel
CVE-2021-34468	No	No	SharePoint Server
CVE-2021-34519	No	No	SharePoint Server
CVE-2021-34469	No	No	Office
CVE-2021-34520	No	No	SharePoint Server

CVE	Public	Exploited	Product
CVE-2021-34451	No	No	Office Online Server
CVE-2021-34517	No	No	SharePoint Server
CVE-2021-31196	No	No	Exchange Server
CVE-2021-31206	No	No	Exchange Server
CVE-2021-31984	No	No	Power BI
CVE-2021-33753	No	No	Bing Search
CVE-2021-33767	No	No	Open Enclave SDK
CVE-2021-34448	No	Yes	Scripting Engine
CVE-2021-34523	Yes	No	Exchange Server
CVE-2021-34473	Yes	No	Exchange Server
CVE-2021-34474	No	No	Dynamics Business Central
CVE-2021-34476	No	No	Bowser.sys
CVE-2021-34528	No	No	Visual Studio Code
CVE-2021-34479	No	No	Visual Studio

CVE	Public	Exploited	Product
CVE-2021-33766	No	No	Exchange
CVE-2021-33768	No	No	Exchange Server
CVE-2021-34470	No	No	Exchange Server
CVE-2021-34477	No	No	Visual Studio Code .NET Runtime
CVE-2021-34529	No	No	Visual Studio Code