Published on *University of Colorado* (https://www.cu.edu)

Security Notices [1]

SEVERE: Microsoft Releases October Updates (October 12, 2021)

Microsoft has released the October updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Products, Features, and Roles

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- .NET Core & Visual Studio
- Active Directory Federation Services
- Console Window Host
- HTTP.sys
- Microsoft DWM Core Library
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Intune
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Rich Text Edit Control
- Role: DNS Server
- Role: Windows Active Directory Server
- Role: Windows AD FSServer
- Role:Windows Hyper-V
- System Center
- Visual Studio
- Windows AppContainer
- Windows AppX Deployment Service
- Windows Bind Filter Driver
- Windows Cloud Files Mini Filter Driver
- Windows Common Log File System Driver
- Windows Desktop Bridge

- Windows DirectX
- Windows Event Tracing
- Windows exFAT File System
- Windows Fastfat Driver
- Windows Installer
- Windows Kernel
- Windows MSHTML Platform
- Windows Nearby Sharing
- Windows Network Address Translation (NAT)
- Windows Print Spooler Components
- Windows Remote Procedure Call Runtime
- Windows Storage Spaces Controller
- Windows TCP/IP
- Windows Text Shaping
- Windows Win32K

Additional Information

Security bulletin name: October 2021 Security Updates
Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct [2]

SEVERE: Microsoft Releases September Updates (September 14, 2021)

Microsoft has released the September updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Products, Features, and Roles

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- Azure Open Management Infrastructure
- Azure Sphere
- Dynamics Business Central Control
- Microsoft Accessibility Insights for Android
- Microsoft Edge (Chromium-based)
- Microsoft Edge forAndroid
- Microsoft MPEG-2 Video Extension
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Microsoft Windows DNS

- Visual Studio
- Windows Ancillary Function Driver forWinSock
- Windows Authenticode
- Windows Bind Filter Driver
- Windows BitLocker
- Windows Common Log File System Driver
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Key Storage Provider
- Windows MSHTML Platform
- Windows Print Spooler Components
- Windows Redirected Drive Buffering
- Windows Scripting
- Windows SMB
- Windows Storage
- Windows Subsystem for Linux
- Windows TDX.sys
- Windows Update
- Windows Win32K
- Windows WLAN Auto Config Service
- Windows WLAN Service

Additional Information

Security bulletin name:September 2021 Security Updates
Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep [3]

SEVERE: Microsoft Releases August Updates (August 10, 2021)

Microsoft has released the August updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Products, Features, and Roles

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- .NET Core & Visual Studio
- ASP .NET
- Azure
- Azure Sphere
- Microsoft Azure Active Directory Connect
- Microsoft Dynamics
- Microsoft Graphics Component
- Microsoft Office

- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Scripting Engine
- Microsoft Windows Codecs Library
- Remote Desktop Client
- Windows Bluetooth Service
- Windows Cryptographic Services
- Windows Defender
- Windows Event Tracing
- Windows Media
- Windows MSHTML Platform
- Windows NTLM
- Windows Print Spooler Components
- Windows Services for NFS ONCRPC XDR Driver
- Windows Storage Spaces Controller
- Windows TCP/IP
- Windows Update
- Windows Update Assistant
- Windows User Profile Service

Additional Information

- Security bulletin name:?August 2021 Security Updates
- Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug [4]

SEVERE: Microsoft Releases Emergency Windows Print Spooler (PrintNightmare) Update (July 7, 2021)

Microsoft has released an emergency update for a Windows Print Spooler service vulnerability that may allow an authenticated remote attacker to take complete control of an affected system. All versions of Windows are vulnerable.

According to CERT/CC, "The Microsoft update only appears to address the Remote Code Execution (RCE via SMB and RPC) variants of the PrintNightmare, and not the Local Privilege Escalation (LPE) variant." [1] You might consider the workarounds until an additional update is released.

Affected Products

The Office of Information Security advises owners of the software listed below to update as soon as possible. Supported versions of Windows that do not have security updates available at this time will be forthcoming.

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)

- Windows Server 2012
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows RT 8.1 Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows Server, version 20H2 (Server Core Installation)
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows Server, version 2004 (Server Core installation)
- Windows 10 Version 2004 for x64-based Systems
- Windows 10 Version 2004 for ARM64-based Systems
- Windows 10 Version 2004 for 32-bit Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

Additional Information

Security bulletin name:

- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527)
- Carnegie Mellon University: CERT/CC Vulnerability Note VU #383432

Learn more about these vulnerabilities:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 [5]
- https://www.kb.cert.org/vuls/id/383432 [6] [1]

SEVERE: Microsoft Releases June Updates (June 8, 2021)

Microsoft has released the June updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Products, Features, and Roles

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- .NET Core & Visual Studio
- 3D Viewer
- Microsoft DWM Core Library
- Microsoft Edge (Chromium-based)
- Microsoft Intune
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft Scripting Engine
- Microsoft Windows Codecs Library
- Paint 3D
- Role: HyperVisual Studio Code - Kubernetes Tools
- Windows Bind Filter Driver
- Windows Common Log File System Driver
- Windows Cryptographic Services
- Windows DCOM Server
- Windows Defender
- Windows Drivers
- Windows Event Logging Service
- Windows Filter Manager
- Windows HTML Platform
- Windows Installer
- Windows Kerberos
- Windows Kernel
- Windows Kernel-Mode Drivers
- Windows Network File System
- Windows NTFS Windows NTLM
- Windows Print Spooler Components

- Windows Remote Desktop
- Windows TCP/IP

Additional Information

- Security bulletin name: June 2021 Security Updates
- Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Jun [7]

SEVERE: Microsoft Releases February Updates (Feb 11, 2021)

Microsoft has released the February updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Products, Features, and Roles

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- .NET Core
- .NET Framework
- Azure IoT
- Developer Tools
- Microsoft Azure Kubernetes Service
- Microsoft Dynamics
- Microsoft Edge for Android
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows Codecs Library
- Role: DNS Server
- Role: Hyper-V
- Role: Windows Fax Service
- Skype for Business
- SysInternals
- System Center
- Visual Studio
- Windows Address Book
- Windows Backup Engine
- Windows Console Driver
- Windows Defender
- Windows DirectX
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Mobile Device Management

- Windows Network File System
- Windows PFX Encryption
- Windows PKU2U
- Windows PowerShell
- Windows Print Spooler Components
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Trust Verification API

Additional Information

Security bulletin name: February 2021 Security Updates
Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb [8]

SEVERE: Microsoft Releases January Updates (Jan 13, 2021)

Microsoft has released the January updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Software

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Visual Studio
- SQL Server
- Microsoft Malware Protection Engine
- .NET Core
- .NET Repository
- ASP .NET
- Azure

Additional Information

Security bulletin name: January 2021 Security Updates
Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan [9]

SEVERE: Microsoft Releases December Updates (Dec 9, 2020)

Microsoft has released the December updates to their software. Some of these updates

address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Software

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge for Android
- ChakraCore
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Exchange Server
- Azure DevOps
- Microsoft Dynamics
- Visual Studio
- Azure SDK
- Azure Sphere

Additional Information

Security bulletin name: December 2020 Security Updates
Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec [10]

SEVERE: Microsoft Releases November Updates (Nov 12, 2020)

Microsoft has released the November updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Software

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- Internet Explorer
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- ChakraCore
- Microsoft Exchange Server
- Microsoft Dynamics
- Microsoft Windows Codecs Library
- Azure Sphere
- Windows Defender
- Microsoft Teams

- Azure SDK
- Azure DevOps
- Visual Studio

Additional Information

- Security bulletin name: November 2020 Security Updates
- Learn more about these vulnerabilities: https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov [11]

SEVERE: Microsoft Releases October Updates (Oct 14, 2020)

Microsoft has released the October updates to their software. Some of these updates address vulnerabilities that may allow a remote attacker to take control of a system.

Affected Software

The Office of Information Security advises owners of the software listed below to update as soon as possible.

- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft JET Database Engine
- Azure Functions
- Open Source Software
- Microsoft Exchange Server
- Visual Studio
- PowerShellGet
- Microsoft .NET Framework
- Microsoft Dynamics
- Adobe Flash Player
- Microsoft Windows Codecs Library

Security Bulletin Name: Release Notes: October 2020 Security Updates

Additional information about these vulnerabilities can be viewed at:
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct [12]

If you have any questions, please contact your campus-specific IT department.

Groups audience:
Office of Information Security
Right Sidebar:
Security Levels
Campus IT Departments

Source URL: https://www.cu.edu/security/notices

Links
[1] https://www.cu.edu/security/notices

[2] https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct
[3] https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep
[4] https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug
[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
[6] https://www.kb.cert.org/vuls/id/383432
[7] https://msrc.microsoft.com/update-guide/releaseNote/2021-Jun
[8] https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb
[9] https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan
[10] https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec
[11] https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov
[12] https://msrc.microsoft.com/update-guide/en-us/releaseNote/2020-Oct