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

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

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 [3]

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

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 [5]

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


Additional information about these vulnerabilities can be viewed at:

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