Date: 2026/05/21

Vulnerability Alert Microsoft Releases May 2026 Security Updates

- Subject: Vulnerability Alert Microsoft Releases May 2026 Security Updates

- Description:
  - Forwarded from National Information Security Analysis Center Cybersecurity Alert NISAC-200-202605-00000007
  - Microsoft has released its May 2026 security updates, patching a total of 139 vulnerabilities. This includes 30 high-risk vulnerabilities and 1 vulnerability that has already been actively exploited. Please confirm and apply the patches as soon as possible.
- Affected Platforms:
  - Products with High-Risk Vulnerabilities
  - ASP.NET Core
  - Azure AI Foundry M365 published agents
  - Azure Cloud Shell
  - Azure Connected Machine Agent
  - Azure DevOps
  - Azure Entra ID
  - Azure Logic Apps
  - Azure Machine Learning
  - Azure Managed Instance for Apache

Cassandra

- Azure Monitor Agent
- Azure Notification Service
- Azure SDK
- Copilot Chat (Microsoft Edge)
- Data Deduplication
- Dynamics Business Central
- GitHub Copilot and Visual Studio
- M365 Copilot
- M365 Copilot for Desktop
- Microsoft Authenticator
- Microsoft Data Formulator
- Microsoft Dynamics 365 Customer Insights
- Microsoft Dynamics 365 (on-premises)
- Microsoft

Edge (Chromium-based)

- Microsoft Edge for Android
- Microsoft Exchange Server

- Microsoft Office
- Microsoft Office Click-To-Run
- Microsoft Office Excel
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Partner Center
- Microsoft SSO Plugin for Jira & Confluence
- Microsoft Teams
- Microsoft Windows DNS
- .NET
- Power Automate
- SQL Server
    - Telnet Client
    - Visual Studio Code
    - Windows Admin Center
    - Windows Ancillary Function Driver for WinSock
    - Windows Application Identity (AppID) Subsystem
    - Windows Cloud Files Mini Filter Driver
    - Windows Common Log File System Driver
    - Windows Cryptographic Services
    - Windows DWM Core Library
    - Windows Event Logging Service
    - Windows Filtering Platform (WFP)
    - Windows GDI
    - Windows Hyper-V
    - Windows Internet Key Exchange (IKE) Protocol
    - Windows Kernel
    - Windows Kernel - Mode Drivers
    - Windows LDAP - Lightweight Directory Access Protocol
    - Windows LLDP
    - Windows Message Queuing
    - Windows Native WiFi Miniport Driver
    - Windows Netlogon
    - Windows Print Spooler Components
    - Windows Projected File System
    - Windows Remote Desktop
    - Windows

Rich Text Edit

- Windows Rich Text Edit Control
- Windows Secure Boot
- Windows SMB Client
- Windows Storage Spaces Controller
- Windows Storport Miniport Driver
- Windows TCP/IP
- Windows Telephony Service
- Windows Volume Manager Extension Driver
- Windows Win32K – GRFX

- Windows Win32K - ICOMP
- Mitigation Measures:
- Official fixes for the vulnerabilities have been released by Microsoft. Organizations can contact their system maintenance vendors or refer to the following link: https://msrc.microsoft.com/update-guide/releaseNote/2026-May
- References:

1. https://msrc.microsoft.com/update-guide/releaseNote/2026-May

---

Computer and Communication Center
Network Systems Division