Post Date: 2026/06/17

【Vulnerability Alert】Microsoft Releases June 2026 Security Updates

- Subject: 【Vulnerability Alert】Microsoft Releases June 2026 Security Updates

- Description:
  - Forwarded from National Information Security Sharing and Analysis Center Security Alert NISAC-200-202606-00000005
  - Microsoft has released its security updates for June 2026, patching a total of 204 vulnerabilities, including 18 high-risk vulnerabilities. Please confirm and apply the patches as soon as possible.
  - 【Products with High-Risk Vulnerabilities】
  - Active Directory Domain Services
  - Azure HorizonDB
  - Azure Stack Edge
  - Microsoft Azure Kubernetes Service
  - Microsoft Dynamics 365 (on-premises)
  - Microsoft Exchange Online
  - Microsoft Exchange Server
  - Microsoft Office SharePoint
  - Nuance PowerScribe
  - Remote Desktop

Client

- Visual Studio Code
- Windows DHCP Client
- Windows DHCP Server
- Windows HTTP.sys
- Windows Kernel
- Windows TCP/IP
- 【Other Affected Products】
- .NET
- ASP.NET Core
- Copilot Chat (Microsoft Edge)
- Function Discovery Service (fdwsd.dll)
- GitHub Copilot and Visual Studio Code
- HTTP/2
- Linux MANA Driver
- M365 Copilot

- Microsoft Azure Attestation service and Device Health Attestation Service
  - Microsoft Bing
  - Microsoft Copilot
  - Microsoft Defender for Endpoint
  - Microsoft Graph

    - Microsoft Graphics Component
    - Microsoft Kinect
    - Microsoft Live Share Canvas SDK
    - Microsoft Office
    - Microsoft Office Click-To-Run
    - Microsoft Office Excel
    - Microsoft Office Project
    - Microsoft Office Word
    - Microsoft

PC Manager

- Microsoft PowerToys
- Microsoft Teams for Android
- Microsoft UxTheme Library (uxtheme.dll)
- Microsoft Windows DNS
- Office for Android
- Role: Windows Hyper-V
- UI Automation Manager (uiamanager.dll)
- Universal Plug and Play (upnp.dll)
- Windows Administrator Protection
- Windows Ancillary Function Driver for WinSock
- Windows Application Identity (AppID) Subsystem
- Windows BitLocker
- Windows Bluetooth

Port Driver

- Windows Bluetooth Service
- Windows Boot Manager
- Windows Collaborative Translation Framework
- Windows Common Log File System Driver
- Windows Cryptographic Services
- Windows Deployment Services
- Windows DWM Core Library
- Windows Hotpatch Monitoring Service
- Windows Hyper-V
- Windows Internet (wininet.dll)
- Windows Kerberos
- Windows Kernel-Mode Drivers
- Windows Mark of the Web (MOTW)

- Windows Media
    - Windows Narrator Braille
    - Windows Network Controller (NC) Host Agent
    - Windows NT OS Kernel
    - Windows NTFS
    - Windows NTLM
    - Windows Performance Monitor
    - Windows Program Compatibility Assistant Service
    - Windows Projected File System Filter Driver

    - Windows Push Notifications
    - Windows RDP
    - Windows SDK
    - Windows Secure Boot
    - Windows

Shell

- Windows Storage
- Windows Telephony Service
- Windows UEFI
- Windows Universal Disk Format File System Driver (UDFS)
- Windows Win32K - GRFX
- Winlogon
- Affected Platforms:
- Active Directory Domain Services
- Azure HorizonDB
- Azure Stack Edge
- Microsoft Azure Kubernetes Service
- Microsoft Dynamics 365 (on-premises)
- Microsoft Exchange Online
- Microsoft Exchange Server
- Microsoft Office SharePoint
- Nuance PowerScribe
- Remote Desktop Client
- Visual Studio Code
- Windows DHCP Client
- Windows DHCP Server
- Windows HTTP.sys
- Windows Kernel
- Windows TCP/IP
- Action Required:
- Microsoft has officially released security patches for these vulnerabilities. Organizations are advised to contact their system maintenance vendors or refer to the following link: https://msrc.microsoft.com/update-guide/releaseNote/2026-Jun
- References:

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

---

Computer and Communication Center
Network Systems Division