مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Microsoft

Tracking #:432319104

Date:10-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has released its June 2026 Patch Tuesday security updates addressing 206 vulnerabilities in its products.

TECHNICAL DETAILS:

Microsoft has released its June 2026 Patch Tuesday security updates addressing 206 vulnerabilities across Windows, Microsoft Office, Outlook, Hyper-V, Remote Desktop Client, BitLocker, HTTP.sys, Microsoft Defender, and other core components.

The release includes:

- 3 publicly disclosed zero-day vulnerabilities
- 37 Critical vulnerabilities
- 166 Important/Moderate vulnerabilities
- Multiple Remote Code Execution (RCE) vulnerabilities
- Several Elevation of Privilege (EoP) vulnerabilities
- Security Feature Bypass vulnerabilities affecting BitLocker
- A publicly disclosed HTTP/2 Denial-of-Service vulnerability
- A Microsoft Defender vulnerability that has been actively exploited in the wild

Organizations should prioritize patching internet-facing systems, remote access infrastructure, domain-joined endpoints, privileged workstations, and systems running Remote Desktop Client.

Publicly disclosed zero-day vulnerabilities

- CVE-2026-50507 – Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2026-49160 – HTTP.sys Denial of Service Vulnerability
- CVE-2026-45586 – Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege

Other Important Vulnerability Details

- CVE-2026-45585 – Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2026-41091 – Microsoft Defender Elevation of Privilege Vulnerability
  - Status: Actively Exploited in the Wild
- CVE-2026-45461 – Microsoft Office Remote Code Execution Vulnerability
- CVE-2026-45463 – Microsoft Office Remote Code Execution Vulnerability
- CVE-2026-45472 – Microsoft Office Remote Code Execution Vulnerability
- CVE-2026-45474 – Microsoft Office Remote Code Execution Vulnerability
- CVE-2026-26142 – Nuance PowerScribe Remote Code Execution Vulnerability
- CVE-2025-10263 – ARM Kernel Elevation of Privilege Vulnerability
- CVE-2026-33828 – Windows Device Health Attestation Elevation of Privilege Vulnerability
- CVE-2026-45456 – Microsoft Outlook and Word Remote Code Execution Vulnerability
- CVE-2026-47635 – Microsoft Outlook and Word Remote Code Execution Vulnerability
- CVE-2026-45458 – Microsoft Outlook and Word Remote Code Execution Vulnerability
- CVE-2026-45460 – Microsoft Office Information Disclosure Vulnerability
- CVE-2026-45607 – Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2026-47652 – Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2026-45641 – Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2026-45648 – Windows Active Directory Domain Services Remote Code Execution Vulnerability

- CVE-2026-45657 – Windows Kernel Remote Code Execution Vulnerability
- CVE-2026-47288 – Windows Kerberos Key Distribution Center (KDC) Remote Code Execution Vulnerability
- CVE-2026-47289 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-47654 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-42992 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-44799 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-44801 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-42985 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-48563 – Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-32193 – Azure Kubernetes Service (AKS) Remote Code Execution Vulnerability
- CVE-2026-45476 – Microsoft Azure Network Adapter Elevation of Privilege Vulnerability
- CVE-2026-48574 – Windows Media Remote Code Execution Vulnerability
- CVE-2026-44810 – Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2026-44815 – DHCP Client Service Remote Code Execution Vulnerability
- CVE-2026-42987 – Windows Deployment Services (WDS) Remote Code Execution Vulnerability
- CVE-2026-44803 – Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2026-44812 – Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2026-47291 – HTTP.sys Remote Code Execution Vulnerability

Note: Refer to the Microsoft June 2026 release notes for the full list of CVEs and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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