مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Microsoft

Tracking #:432317364

Date:11-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has released security updates to patch multiple vulnerabilities in its products including an actively exploited zero-day vulnerability.

TECHNICAL DETAILS:

Microsoft's June 2025 Patch Tuesday fixes 66 vulnerabilities, including two zero-days in WebDAV (CVE-2025-33053) and Chromium V8 (CVE-2025-5419). Also addressed ten critical flaws enable remote code execution or privilege escalation, with patches issued even for legacy systems.

Zero-Day Vulnerability: Among these, two zero-day vulnerabilities ,one already exploited in the wild and the other publicly disclosed.

- CVE-2025-33053 – A remote code execution flaw in WebDAV- Actively exploited
- CVE-2025-5419 – A memory corruption issue in the Chromium V8 JavaScript engine used by Microsoft Edge

Critical Vulnerabilities:

Microsoft Office – Preview Pane Exploitable

CVE	CVSS	Description
CVE-2025-47162	8.4	Heap-based buffer overflow
CVE-2025-47164	8.4	Use-after-free
CVE-2025-47167	8.4	Type confusion
CVE-2025-47953	8.4	Improper resource restriction

Windows Core Components

CVE	CVSS	Component	Description
CVE-2025-33070	8.1	Netlogon	Privilege escalation to domain admin via uninitialized memory
CVE-2025-29828	8.1	Schannel (TLS)	RCE via memory leak during handshake
CVE-2025-32710	8.1	Remote Desktop Gateway	RCE via race condition & use-after-free
CVE-2025-33071	8.1	KDC Proxy Service	RCE via race condition in Kerberos Proxy
CVE-2025-47172	8.8	SharePoint Server	RCE via authenticated SQL injection

Other High-Risk Important Vulnerabilities (Under Exploitation or Public Disclosure)

- CVE-2025-33073-8.8-Windows SMB Client Elevation of privilege via network exploit. Public PoC exists. SYSTEM-level access possible. No user interaction required.

RECOMMENDATIONS:

- Immediately prioritize patching the actively exploited zero-day vulnerability CVE-2025-33053 (WebDAV RCE), especially on internet-facing servers.

- Apply updates for all Microsoft Office products, especially in environments using Preview Pane, to mitigate other Critical RCE vulnerabilities exploitable via email or documents.

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/2025-Jun