مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates July- Microsoft

Tracking #:432317469

Date:09-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

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 a publicly disclosed zero-day vulnerability.

TECHNICAL DETAILS:

Microsoft's July 2025 Patch Tuesday addresses 137 security vulnerabilities, including a publicly disclosed zero-day vulnerability in Microsoft SQL Server and 14 Critical vulnerabilities, 10 of which are Remote Code Execution (RCE) flaws. These vulnerabilities impact widely used Microsoft products such as SQL Server, Office, SharePoint, and Windows OS components. Immediate action is recommended, especially for enterprise environments running SQL Server or Microsoft Office.

This month’s patches also include mitigations for two AMD side-channel vulnerabilities and a variety of elevation of privilege, information disclosure, denial of service, spoofing, and security feature bypass flaws.

Zero-Day Vulnerability:
CVE-2025-49719 – Microsoft SQL Server Information Disclosure

- **Type:** Information Disclosure
- **Impact:** Unauthorized disclosure of data via uninitialized memory
- **Attack Vector:** Remote, unauthenticated attacker
- **Fix:** Install latest SQL Server updates and Microsoft OLE DB Driver 18 or 19

Critical Vulnerabilities:

Windows SPNEGO

- CVE-2025-47981 – Critical – SPNEGO Extended Negotiation (NEGOEX) RCE – CVSS 9.8

Microsoft Office & SharePoint

- CVE-2025-49704 – Critical – Microsoft SharePoint RCE – CVSS 8.8
- CVE-2025-49695 – Critical – Microsoft Office RCE – CVSS 8.4
- CVE-2025-49696 – Critical – Microsoft Office RCE – CVSS 8.4
- CVE-2025-49697 – Critical – Microsoft Office RCE – CVSS 8.4
- CVE-2025-49698 – Critical – Microsoft Word RCE – CVSS 7.8
- CVE-2025-49702 – Critical – Microsoft Office RCE – CVSS 7.8
- CVE-2025-49703 – Critical – Microsoft Word RCE – CVSS 7.8

Windows Hyper-V

- CVE-2025-48822 – Critical – Hyper-V DDA RCE – CVSS 8.6
- CVE-2025-29828 – Critical – Hyper-V DDA RCE – CVSS 8.1

Microsoft SQL Server

- CVE-2025-49717 – Critical – SQL Server RCE – CVSS 8.5

Windows KPSSVC (Kerberos KDC Proxy)

- CVE-2025-49735 – Critical – KPSSVC RCE – CVSS 8.1

Microsoft Imaging Component

- CVE-2025-47980 – Critical – Imaging Component Info Disclosure – CVSS 6.2

AMD CPU Vulnerabilities

- CVE-2025-36350 – Critical – AMD Store Queue Info Disclosure – CVSS 5.6
- CVE-2025-36357 – Critical – AMD L1 Data Queue Info Disclosure – CVSS 5.6

RECOMMENDATIONS:

- Immediately patch systems running Microsoft SQL Server, applying both the latest SQL Server update and the Microsoft OLE DB Driver 18 or 19 to address the CVE-2025-49719 zero-day.
- Prioritize patching Microsoft Office, especially on systems exposed to untrusted document sources. Users are vulnerable even through Preview Pane functionality.
- Monitor for updates if using Microsoft Office LTSC for Mac 2021 or 2024, as security updates are pending release.
- Apply updates to Microsoft SharePoint to address CVE-2025-49704, a critical RCE flaw exploitable over the Internet by authenticated users.
- Consider reviewing environment for exposure to AMD side-channel vulnerabilities, especially in virtualized or shared environments.
- Conduct vulnerability scans and audit patch compliance across systems.

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-Jul