مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-Microsoft

Tracking #:432317816

Date:15-10-2025

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 Microsoft has released a substantial security update addressing 172 vulnerabilities across its products, including six zero-day vulnerabilities and three actively exploited vulnerabilities.

TECHNICAL DETAILS:

Microsoft has released its October 2025 Patch Tuesday security updates, addressing 172 vulnerabilities across multiple products and components. The release includes six zero-day vulnerabilities, eight critical-rated issues, and a broad range of privilege escalation, information disclosure, and remote code execution flaws. This month's release is particularly critical due to the active exploitation of three flaws.

Actively exploited zero-day vulnerabilities
The following vulnerabilities are being actively exploited in the wild and require immediate patching.

1. CVE-2025-24990 – Windows Agere Modem Driver Elevation of Privilege
   - Type: Elevation of Privilege (EoP)
   - Impact: Local privilege escalation to SYSTEM
   - Description: Vulnerability in the Agere Modem driver (ltmdm64.sys) allows attackers to gain administrative privileges.

2. CVE-2025-47827 – Secure Boot Bypass in IGEL OS
   - Type: Secure Boot Bypass
   - Impact: Allows mounting unverified root filesystems leading to Secure Boot compromise
   - Description: In IGEL OS before version 11, improper signature verification in igel-flash-driver allows a crafted image to bypass Secure Boot.

3. CVE-2025-59230 – Windows Remote Access Connection Manager EoP
   - Type: Elevation of Privilege
   - Impact: SYSTEM-level access through improper access control
   - Description: A local attacker could elevate privileges by exploiting improper permission handling in Remote Access Connection Manager (RasMan)

Other Zero Day Vulnerabilities:

1. CVE-2025-24052 – Windows Agere Modem Driver Elevation of Privilege
   - Type: EoP
   - Impact: Affects all supported Windows versions, exploitable even if the modem is not in use.
   - Description: Similar to CVE-2025-24990, publicly disclosed flaw in the same driver class.

2. CVE-2025-0033 – AMD EPYC Processors SEV-SNP Race Condition
   - Type: Information Disclosure / Integrity Impact
   - Impact: Potential compromise of SEV-SNP protected memory integrity during RMP initialization.
   - Description: A race condition during Secure Nested Paging (SNP) initialization may allow a privileged attacker to alter RMP entries.

3. CVE-2025-2884 – TPM 2.0 Out-of-Bounds Read
    - Type: Information Disclosure / DoS
    - Impact: Could expose TPM data or cause denial of service.
    - Description: The Trusted Computing Group (TCG) TPM 2.0 reference implementation has an out-of-bounds read in CryptHmacSign due to improper validation of signature schemes.

RECOMMENDATIONS:

1. Prioritize patching the actively exploited zero-day vulnerabilities immediately.
2. Expedite patching for all critical vulnerabilities, especially those rated as "Exploitation More Likely" by Microsoft.
3. Deploy all remaining security updates in a timely manner as per organization's patch management policy**.**

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-Oct