مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Microsoft

Tracking #:432316859

Date:12-02-2025

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Microsoft has released security updates addressing 67 vulnerabilities across multiple products as part of its February 2025 Patch updates. This includes four zero-day vulnerabilities, two of which have been actively exploited in the wild.

Actively Exploited Zero-Day Vulnerabilities:

- **CVE-2025-21391 - Windows Storage Elevation of Privilege Vulnerability:** This vulnerability allows attackers to delete targeted files, potentially disrupting services. While it doesn't expose confidential information, data deletion can lead to service unavailability.
- **CVE-2025-21418 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability:** This critical vulnerability allows attackers to gain SYSTEM privileges on affected Windows systems. This level of access grants complete control over the compromised machine.

Publicly Disclosed Zero-Day Vulnerabilities:

- **CVE-2025-21194 - Microsoft Surface Security Feature Bypass Vulnerability:** This hypervisor vulnerability can allow attackers to bypass UEFI and compromise the secure kernel on certain hardware, potentially impacting virtual machines.
- **CVE-2025-21377 - NTLM Hash Disclosure Spoofing Vulnerability:** This vulnerability can expose Windows user NTLM hashes, potentially allowing remote attackers to impersonate users. Minimal user interaction with a malicious file can trigger this vulnerability.

Critical Severity Vulnerability:

- **CVE-2025-21198 - Microsoft High Performance Compute (HPC) Pack Remote Code Execution Vulnerability:** This vulnerability allows for remote code execution on systems running HPC Pack, potentially giving attackers control over these systems.

Other Notable Flaws:

- **CVE-2025-21376 - Windows LDAP Remote Code Execution Vulnerability:** This vulnerability in LDAP could allow unauthenticated attackers to execute arbitrary code. While exploitation requires a race condition, the potential impact on network authentication and directory services is severe.
- **CVE-2025-21381 - Microsoft Excel Remote Code Execution Vulnerability:** This vulnerability could allow attackers to execute code remotely via crafted Excel files. Given the widespread use of Excel, this poses a significant risk.

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/2025-Feb