مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Microsoft

Tracking #:432316743

Date:15-01-2025

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 for January 2025, addressing 159 vulnerabilities, including eight zero-day vulnerabilities, with three actively exploited in the wild. This update is crucial for maintaining system security and should be applied promptly.

Zero-Day Vulnerabilities:
Actively Exploited Zero-Days:

- **CVE-2025-21333**
- **CVE-2025-21334**
- **CVE-2025-21335**

Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerabilities, allowing attackers to gain SYSTEM privileges on Windows devices. The flaws affect a component of Windows Hyper-V's NT Kernel that manages communication between virtual machines and the host operating system.

Publicly Disclosed Zero-Days:

- **CVE-2025-21275**: Windows App Package Installer Elevation of Privilege Vulnerability
- **CVE-2025-21308**: Windows Themes Spoofing Vulnerability.
- **CVE-2025-21186, CVE-2025-21366, CVE-2025-21395:** Microsoft Access Remote Code Execution Vulnerabilities.

Critical Severity Vulnerabilities:

- Windows OLE (**CVE-2025-21298**): This remote code execution vulnerability affects Windows Object Linking and Embedding (OLE). An attacker could exploit it by sending a specially crafted email to a target using a vulnerable version of Microsoft Outlook. Even previewing the malicious email could trigger the exploit, potentially allowing remote code execution on the victim's system
- Reliable Multicast Transport Driver (**CVE-2025-21307**): This vulnerability impacts the Windows Reliable Multicast Transport Driver (RMCAST). It can be exploited if an application is actively listening on a port for Pragmatic General Multicast (PGM). An unauthenticated attacker could send specially crafted packets to an open PGM socket on a Windows server, potentially executing remote code.
- Windows NTLM (**CVE-2025-21311**): This vulnerability affects the Windows NTLMv1 protocol, allowing attackers to gain elevated privileges on affected systems. The flaw lies in NTLMv1's weaker cryptographic practices, making it easier for attackers to intercept or tamper with authentication processes and escalate their privileges

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-Jan