مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Microsoft

Tracking #:432318116

Date:10-12-2025

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 its December 2025 security updates, addressing 57 vulnerabilities across the Windows ecosystem and associated Microsoft products, including one actively exploited zero-day and two publicly disclosed zero-day vulnerabilities.

Zero-Day Vulnerabilities (3 Total — 1 Actively Exploited, 2 Publicly Disclosed)

1. Actively Exploited Zero-Day

- **CVE-2025-62221 — Windows Cloud Files Mini Filter Driver Elevation of Privilege**
- **Severity:** High
- A use-after-free flaw in the Windows Cloud Files Mini Filter Driver allows an authenticated attacker to elevate privileges to SYSTEM.
- Successful exploitation allows an attacker with local access to **elevate privileges to SYSTEM**, enabling full control over the affected system.

2. Publicly Disclosed Zero-Day

- **CVE-2025-64671 — GitHub Copilot for JetBrains Remote Code Execution**
- **Severity:** High
- A command injection flaw in **GitHub Copilot for JetBrains IDEs** allows unauthorized local code execution.
- The vulnerability stems from **improper neutralization of special command elements**, enabling attackers to append malicious commands to those auto-approved in the user's terminal.

3. Publicly Disclosed Zero-Day

- **CVE-2025-54100 — PowerShell Remote Code Execution**
- **Severity:** High
- A command injection issue in **Windows PowerShell** could cause embedded scripts in a webpage to execute when retrieved using Invoke-WebRequest.
- Attackers could exploit this flaw to run arbitrary commands locally.

Other Notable Remote Code Execution Vulnerabilities

- CVE-2025-62554 — Microsoft Office RCE
- CVE-2025-62557 — Microsoft Office RCE
- CVE-2025-62562 — Microsoft Outlook RCE

Impact

Exploitation of these vulnerabilities could enable:

- Full system compromise via RCE
- Privilege escalation to SYSTEM level
- Unauthorized code execution originating from malicious files, web content, or injected commands
- Lateral movement across enterprise networks

- Initial foothold for ransomware or APT operations

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-Dec