مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of Windows Shell Spoofing Vulnerability

Tracking #:432318858

Date:29-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has confirmed active exploitation of a Windows Shell vulnerability tracked as CVE-2026-32202, originally released on April 14, 2026 and updated on April 27, 2026.

TECHNICAL DETAILS:

Microsoft has confirmed active exploitation of a Windows Shell vulnerability tracked as CVE-2026-32202, originally released on April 14, 2026 and updated on April 27, 2026.This vulnerability is classified as a Protection Mechanism Failure (CWE-693) that enables spoofing attacks over a network. Although the CVSS score is relatively low (4.3), the fact that exploitation is observed in the wild elevates its operational risk.
The flaw requires user interaction—specifically, executing a malicious file—and may allow attackers to expose limited sensitive information without impacting system integrity or availability.

Vulnerability Details:

- CVE ID: **CVE-2026-32202**
- Component: Windows Shell
- Vendor: Microsoft
- Weakness: CWE-693
- Impact Type: Spoofing
- Severity: Important (CVSS 4.3)
- Exploitation Status: **Actively exploited**

CVSS v3.1 Vector

- AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Attack Characteristics

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: Required (execution of malicious file)
- Scope: Unchanged

Exploit Insights

- Exploitation involves delivering a crafted malicious file to the victim.
- Successful execution leads to spoofed content presentation via Windows Shell.
- Reportedly linked to an incomplete patch for CVE-2026-21510, enabling bypass conditions.
- Exploit Code Maturity: Functional
- Remediation Level: Official patch available
- Exploit Status: Confirmed in the wild

RECOMMENDATIONS:

Immediate Actions

- **Apply Security Updates**
  - Deploy April 2026 Patch Tuesday updates from Microsoft without delay.

- **Endpoint Protection**
  - Ensure EDR/XDR solutions are updated to detect spoofed file execution patterns.

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/vulnerability/CVE-2026-32202