مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Zero-Day Vulnerability in Microsoft Office

Tracking #:432318314

Date:27-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft released emergency out-of-band security updates to address a high-severity security feature bypass vulnerability in Microsoft Office that is actively exploited in the wild.

TECHNICAL DETAILS:

Microsoft released emergency out-of-band security updates on January 26, 2026, to address CVE-2026-21509, a high-severity security feature bypass vulnerability in Microsoft Office that is actively exploited in the wild. The flaw allows attackers to bypass OLE (Object Linking and Embedding) mitigations designed to block unsafe COM (Component Object Model) and OLE controls in malicious Office documents. Exploitation requires user interaction (opening a crafted file) but has low complexity and can lead to high impact on confidentiality, integrity, and availability (CVSS v3.1:7.8).

Affected products include Microsoft Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024, and Microsoft 365 Apps for Enterprise. For Office 2021 and later versions, protection is provided via a service-side change (requires restarting Office applications). Security updates are available for all affected versions, including Office 2016 and 2019. Organizations should prioritize patching immediately. As an interim measure for unpatched Office 2016/2019 systems, apply the provided registry-based workaround to block the vulnerable COM object. This vulnerability underscores ongoing risks from legacy COM/OLE components and social engineering via weaponized documents.

Vulnerability Details

- **CVE ID**: CVE-2026-21509
- **CVSS v3.1 Base Score**: 7.8 (High)
- **Title**: Microsoft Office Security Feature Bypass Vulnerability
- **Published**: January 26, 2026
- **Weakness**: CWE-807: Reliance on Untrusted Inputs in a Security Decision
- **Description**: Reliance on untrusted inputs in a security decision allows an unauthorized attacker to bypass a security feature locally. Specifically, the vulnerability bypasses OLE mitigations in Microsoft Office and Microsoft 365 that protect users from vulnerable COM/OLE controls.
- **Attack Vector**: Local (AV:L)
- **Attack Complexity**: Low (AC:L)
- **Privileges Required**: None (PR:N)
- **User Interaction**: Required (UI:R) – Attacker must send a malicious Office file and convince the user to open it
- **Exploitation Status**: Actively exploited (Exploitation Detected)
- **Attack Requirements**: Social engineering to deliver and open a malicious Office document containing exploited COM/OLE element.

Affected Products

- Microsoft Office 2016
- Microsoft Office 2019
- Microsoft Office LTSC 2021
- Microsoft Office LTSC 2024
- Microsoft 365 Apps for Enterprise

RECOMMENDATIONS:

Immediate Actions:

- Apply Microsoft security updates immediately, prioritizing Office 2016 and 2019 systems.
- Restart Office applications to ensure service-side protections are active.
- Deploy interim registry mitigation only if patching cannot be completed promptly.

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-2026-21509