THREAT ADVISORY

Zero-Day Microsoft Office Security Feature Bypass

CVE-2026-21509

January 27, 2026

Executive Summary

Microsoft released an emergency out-of-band security update to address CVE-2026-21509, a high-severity zero-day vulnerability affecting multiple versions of Microsoft Office. The vulnerability allows attackers to bypass critical security features (specifically OLE mitigations) and is currently being actively exploited in the wild.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added this flaw to its Known Exploited Vulnerabilities (KEV) catalog on January 26, 2026, mandating federal agencies to patch by February 16, 2026.

Vulnerability Details

- CVE ID: CVE-2026-21509
- CVSS Score: 7.8 (High)
- Vulnerability Type: Security Feature Bypass
- **Affected Products**:
    - Microsoft Office 2016 (32-bit & 64-bit)
    - Microsoft Office 2019 (32-bit & 64-bit)
    - Microsoft Office LTSC 2021 & 2024
    - Microsoft 365 Apps for Enterprise

Operational Intelligence & Attack Vector

- **Attack Vector**: The vulnerability is triggered when a user opens a specially crafted, malicious Office file. It relies on untrusted inputs to bypass checks that usually prevent dangerous Object Linking and Embedding (OLE) controls from running.
- **User Interaction**: Required. The user must be convinced to open the file (phishing/social engineering).
- **Preview Pane**: Microsoft has confirmed the Preview Pane is not an attack vector.
- **Active Exploitation**: Confirmed by Microsoft Threat Intelligence Center (MSTIC) and CISA. While specific threat actor attribution is currently limited, the immediate addition to the CISA KEV catalog indicates reliable evidence of attacks.

Mitigation & Remediation

Microsoft issued different remediation paths depending on the Office version:

1. **Modern Versions** (**Office 2021, LTSC, Microsoft 365**)

- **Action**: These versions are protected via a service-side update (Experimentation and Configuration Service - ECS).
- **Requirement**: Users must restart their Office applications for the protection to take effect.

2. **Older Versions** (**Office 2016, 2019**)

- **Action**: Administrators must manually install the out-of-band security updates released on January 26/27.
    - *Office 2016:* KB5002573
    - *Office 2019:* Build 10417.20095

3. **Registry Workaround** (**Temporary**)

If patching is not immediately possible, Microsoft has provided a registry modification to disable the vulnerable functionality. *Note: Backup the registry before modifying.*

- **Path**: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\COM Compatibility\{EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}
- **Value**: Compatibility Flags (REG_DWORD) = 0x00000400

Recommendations

1. **Immediate Patching**: Prioritize patching Office 2016 and 2019 instances, as they do not receive the automatic service-side fix.
2. **Force Restarts**: Issue a communication or policy to force-restart Office applications for Microsoft 365/2021 users to ensure the service-side mitigation is applied.
3. **Phishing Awareness**: Alert users to be hyper-vigilant regarding unsolicited Office attachments, even from known contacts, due to the required user interaction component.
4. **Threat Hunting**: Monitor for the creation of the specific registry keys mentioned above if they were not implemented by IT, as attackers sometimes modify COM compatibility flags to facilitate persistence or bypasses.