UPDATE - Active Exploitation of Microsoft Office Zero-Day Bypasses Security Protections

TL;DR

Microsoft confirmed active exploitation of a Microsoft Office zero-day, CVE-2026-21509, that lets attackers bypass built-in security protections using a malicious Office file.

Office 2021 and newer are protected through a service-side fix after a restart. Fixes for Office 2016 and 2019 are not yet available. Until they are, Microsoft recommends applying the registry-based mitigation.

UPDATE – 1/27/2026

Microsoft released security updates for CVE-2026-21509. Office 2021, Office LTSC 2024, and Microsoft 365 Apps receive the fix through a service-side update that takes effect after restarting Office applications. Security updates for Office 2016 and Office 2019 are not yet available, and Microsoft stated patches for those versions will be released as soon as possible.

Mitigations and Guidance

- Restart Office applications on Office 2021, LTSC 2024, and Microsoft 365 to apply the service-side fix
- Apply Microsoft's registry-based mitigation on Office 2016 and 2019 systems until patches are released
- Keep Protected View and Microsoft Defender protections enabled
- Avoid opening Office files from unknown or untrusted sources

---

Overview

Microsoft released out-of-band updates to address an actively exploited security feature bypass affecting Microsoft Office. Tracked as CVE-2026-21509 (CVSS 7.8), the vulnerability allows attackers to bypass OLE mitigation controls designed to block unsafe COM/OLE objects. Microsoft confirmed exploitation in the wild.

The attack requires user interaction. An attacker must deliver a malicious Office document and convince the user to open it. The Preview Pane is not involved, but once the file is opened, Office's protective controls can be bypassed locally.

Impacted Products

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

Microsoft applied a service-side fix for Office 2021, LTSC 2024, and Microsoft 365 Apps. Users on these versions are protected after restarting Office applications.

Security updates for Office 2016 and 2019 are not yet available. Microsoft has stated patches for these versions will be released as soon as possible. Office is a reliable delivery path for attackers because it depends on routine user behavior. This vulnerability bypasses a core safety control meant to stop unsafe object handling. Environments running older Office versions are at risk during the patch gap, especially where document-based workflows are common.

Aspire Protects

- **Patch** – Restart Office applications on Office 2021, LTSC 2024, and Microsoft 365 to activate protection
- Apply the registry mitigation on Office 2016 and 2019 systems
- Restrict exposure to untrusted Office documents
- Prepare to deploy patches for Office 2016 and 2019 as soon as Microsoft releases them

TTPs

Initial Access

- Phishing [T1566] – The attacker may deliver a malicious Microsoft Office document to the user to initiate exploitation.

Execution

- User Execution [T1204] – The attacker may require the user to open the malicious Office file for the vulnerability to be triggered.

Defense Evasion

- Exploitation for Defense Evasion [T1211] – The attacker may have bypassed Microsoft Office OLE security mitigations designed to block unsafe COM/OLE controls.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This Microsoft Office zero-day impacts any organization that relies on Office documents as part of daily business operations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-21509 - Security Update Guide - Microsoft - Microsoft Office Security Feature Bypass Vulnerability