Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-21509: Microsoft Office Zero-Day Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
January 27, 2026	A1	TA2026023

Summary

First Seen: January 26, 2026
Affected Products: Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise
Impact: CVE-2026-21509 is a high-severity Security Feature Bypass vulnerability in Microsoft Office that allows attackers to circumvent built-in OLE security protections through maliciously crafted documents. The flaw affects multiple Office versions, including Microsoft 365 Apps and Office 2016–LTSC 2024, and has been confirmed as actively exploited in zero-day attacks. Exploitation requires user interaction, typically via phishing emails delivering malicious Office files. Microsoft has released service-side mitigations and security updates, and organizations should prioritize patching and reinforce controls against malicious email attachments.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office	✓	✓	✓

Vulnerability Details

#1

CVE-2026-21509 is a Security Feature Bypass vulnerability affecting Microsoft Office, the widely used productivity suite that includes Word, Excel, PowerPoint, and related applications. The issue impacts multiple versions, including Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024, and Microsoft 365 Apps, and carries a CVSS v3.1 score of 7.8 (High).

#2

The vulnerability arises from Office's reliance on untrusted input during security-critical decision making, allowing attackers to locally bypass Object Linking and Embedding (OLE) mitigations. Due to improper input validation, Office may fail to correctly enforce built-in security protections, enabling malicious embedded objects to evade safeguards intended to prevent unsafe content from being processed or executed.

#3

The vulnerability has been confirmed as actively exploited in the wild. Microsoft's Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), and the Office Product Group Security Team have been credited with identifying the issue. Exploitation requires user interaction, typically through phishing emails delivering malicious Office documents that must be opened by the victim. The flaw was exploited as a zero-day prior to patch release, indicating that at least one threat actor possessed a functional exploit.

#4

Microsoft has released service-side mitigations and security updates to address the vulnerability. Users running Office 2021 and later are automatically protected after restarting Office applications, while Office 2016 and 2019 users must ensure the relevant updates are installed. A registry-based mitigation is also available as an alternative. Organizations should prioritize patch deployment and reinforce user awareness to mitigate the risk posed by malicious Office attachments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-21509	Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	CWE-807

Recommendations

Apply Microsoft Security Updates Immediately: Install the emergency security updates released by Microsoft for all affected Office versions without delay. Users running Office 2021 and later will be automatically protected via a service-side change but must restart their Office applications for the protection to take effect. Users running Microsoft Office 2016 and 2019 must ensure the update is manually installed to receive protection against this vulnerability.

Implement Registry-Based Mitigation for Unpatched Systems: For systems where immediate patching is not feasible, implement the registry-based workaround detailed in Microsoft's advisory. This involves adding a specific registry subkey that provides protection against exploitation until patches can be deployed. Organizations should document which systems use this temporary mitigation and establish a timeline for full patch deployment.

Enable Automatic Office Updates: Configure Microsoft Office installations across the organization to receive automatic updates. This ensures that future security patches are applied promptly without requiring manual intervention, reducing the window of exposure for newly disclosed vulnerabilities.

Strengthen Email Security Controls: Implement advanced email filtering and sandboxing solutions to detect and block weaponized Office documents before they reach end users. Configure email gateways to quarantine suspicious attachments, particularly those containing macros or embedded OLE objects, for additional security review.

Disable Macros and OLE Controls Where Possible: Evaluate business requirements and disable macros and OLE controls in Office applications where they are not essential for daily operations. Use Group Policy to enforce these restrictions across the organization, significantly reducing the attack surface for Office-based exploitation.

Conduct Security Awareness Training: Educate employees about the risks of opening unsolicited Office documents, particularly those received via email or downloaded from untrusted sources. Emphasize the ongoing threat of phishing campaigns that leverage weaponized documents and reinforce procedures for reporting suspicious emails or files.

Deploy Endpoint Detection and Response Solutions: Ensure that behavioral endpoint detection and response (EDR) capabilities are deployed across all endpoints. Traditional signature-based antivirus may fail to detect zero-day exploitation, making behavioral analysis essential for identifying post-exploitation activities and enabling rapid incident response.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1559: Inter-Process Communication	T1559.001: Component Object Model
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

References

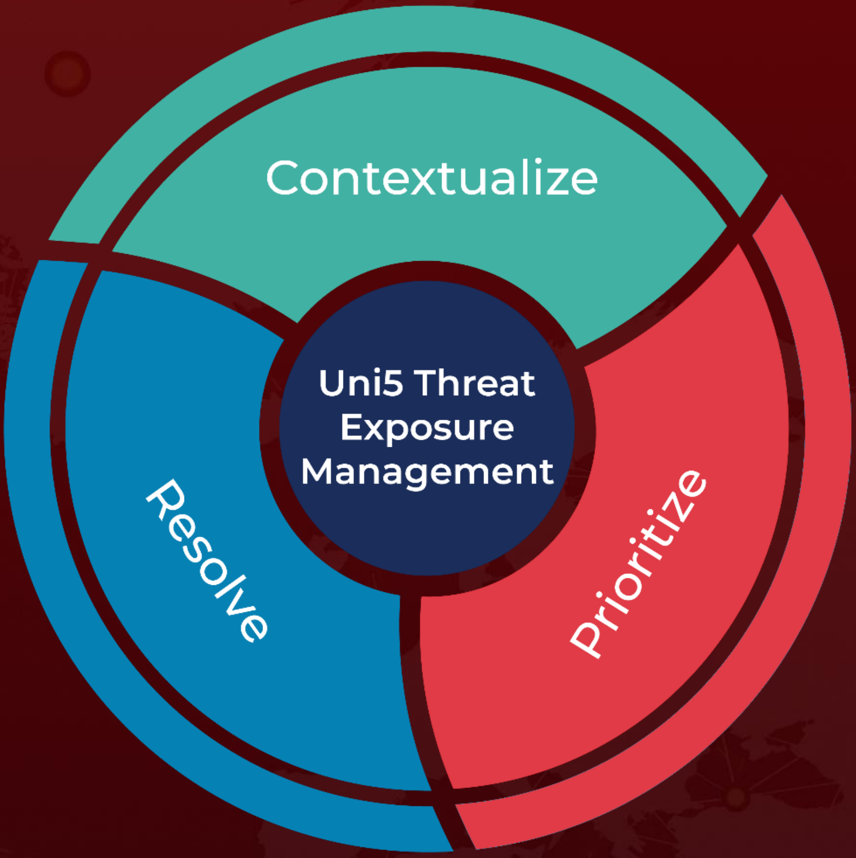
https://www.helpnetsecurity.com/2026/01/27/microsoft-reveals-actively-exploited-office-zero-day-provides-emergency-fix-cve-2026-21509/

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 27, 2026 ● 08:45 AM

More at www.hivepro.com