Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Active Exploitation of CVE-2026-42897 Targets Microsoft Exchange Servers

Date of Publication	Admiralty Code	TA Number
May 18, 2026	A1	TA2026134

Summary

First Seen: May 14, 2026
Affected Products: Microsoft Exchange Server 2016, Microsoft Exchange Server 2019, Microsoft Exchange Server Subscription Edition (SE)
Impact: Microsoft has confirmed active exploitation of CVE-2026-42897, a newly disclosed spoofing vulnerability affecting on-premises Exchange Server deployments. The flaw, rooted in a cross-site scripting (XSS) issue within Outlook Web Access (OWA), allows attackers to embed malicious JavaScript into specially crafted emails that can execute in a victim's authenticated browser session. The vulnerability impacts Exchange Server 2016, 2019, and Subscription Edition (SE), while Exchange Online remains unaffected. Although no permanent patch is currently available, Microsoft has rolled out temporary mitigations through the Exchange Emergency Mitigation Service (EEMS) and the Exchange On-premises Mitigation Tool (EOMT) to help organizations reduce exposure as attacks continue in the wild.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-42897	Microsoft Exchange Server Cross-Site Scripting Vulnerability	Microsoft Exchange Server	✓	✓	✗

Vulnerability Details

#1

CVE-2026-42897 is a spoofing vulnerability caused by a cross-site scripting (XSS) flaw in the web-facing components of on-premises Microsoft Exchange Server. The issue stems from the improper sanitization of user-controlled input embedded within email content before it is rendered in the Outlook Web Access (OWA) interface.

#2

At its core, the vulnerability is linked to inadequate input validation in Exchange Server, allowing attackers to embed malicious JavaScript payloads within specially crafted emails. When a victim accesses the email through OWA and performs certain undisclosed interactions, the injected script executes within the security context of the victim's authenticated browser session. This could enable attackers to hijack sessions, manipulate mailbox data, or conduct further malicious activity while impersonating the user.

#3

Microsoft confirmed that all update levels of Microsoft Exchange Server 2016, Exchange Server 2019, and Exchange Server Subscription Edition (SE) are affected, while Microsoft Exchange Online is not impacted. The company has also marked the flaw as "Exploitation Detected," indicating that the vulnerability is already being actively exploited in the wild.

#4

At present, no permanent security patch has been released. As an interim measure, Microsoft is using the Exchange Emergency Mitigation Service (EEMS) to automatically deploy a URL rewrite rule designed to block exploitation attempts. For air-gapped environments or systems where EEMS cannot be used, administrators can manually apply protections through the Exchange On-premises Mitigation Tool (EOMT). Microsoft has not yet disclosed details about the threat actors behind the attacks, the scope of targeting, or the effectiveness of ongoing exploitation campaigns.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-42897	Microsoft Exchange Server 2016 (all update levels), Microsoft Exchange Server 2019 (all update levels), Microsoft Exchange Server Subscription Edition (all update levels)	cpe:2.3:a:microsoft:exchange_server:2016:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:-:*:*:*:subscription:*:*:*	CWE-79

Recommendations

Enable Exchange Emergency Mitigation Service (EEMS) Immediately: Verify that the Exchange Emergency Mitigation Service is active on all on-premises Exchange Servers. EEMS is enabled by default and will automatically apply a URL rewrite configuration to mitigate CVE-2026-42897. If the Windows service has been disabled, re-enable it without delay. This is the fastest path to reducing exposure while a permanent patch is pending.

Apply Manual Mitigation via EOMT for Air-Gapped Environments: For Exchange Servers operating in air-gapped or isolated networks where EEMS cannot function, download the latest Exchange On-premises Mitigation Tool (EOMT) from Microsoft and execute it via an elevated Exchange Management Shell. Run the command .\EOMT.ps1 -CVE "CVE-2026-42897" on each server individually, or use the pipeline command to apply across all non-Edge servers simultaneously.

Validate Mitigation Application Status: After enabling EEMS or running EOMT, verify that the mitigation status displays as "Applied" on each server. Microsoft has acknowledged a known cosmetic issue where the Description field may display "Mitigation invalid for this exchange version" even when the mitigation has been successfully applied. Confirm application by checking the status field rather than the description.

Restrict OWA Exposure Where Feasible: As a supplemental hardening measure, limit external access to Outlook Web Access through firewall rules, VPN requirements, or conditional access policies until a permanent patch is available. Reducing the attack surface by limiting who can reach OWA from the internet significantly decreases the likelihood of exploitation.

Apply Permanent Patch Upon Release: Monitor Microsoft's Security Response Center (MSRC) and Exchange Team Blog for the release of a cumulative update or security update that permanently addresses CVE-2026-42897. Plan for an expedited patch deployment cycle given the confirmed active exploitation status and CISA KEV listing.

Vulnerability Management: Maintain a continuous vulnerability management program that includes regular scanning of Exchange Server infrastructure, tracking of security advisories from Microsoft and CISA, and prompt evaluation of emergency mitigations. Ensure an accurate inventory of all Exchange Server versions and update levels across the environment, and assess the security posture of email infrastructure as a critical business service.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Defense Evasion	T1036: Masquerading	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

No permanent patch has been released by Microsoft at the time of publication. The following mitigation resources are available:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

References

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

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 Demo of **HivePro**.

REPORT GENERATED ON

May 18, 2026 • 9:00 AM

More at www.hivepro.com