

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

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

Date of Publication

May 18, 2026

Last Update Date

June 11, 2026

Admiralty Code

A1

TA Number

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. Microsoft strongly advises that organizations install the June 2026 Security Updates for their version of Exchange Server as soon as possible to protect against this vulnerability and to help reduce exposure as attacks continue to occur 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

Microsoft advises installing the June 2026 Security Updates for your version of Exchange Server as soon as possible to protect against this vulnerability. As a temporary measure, Microsoft is utilizing the Exchange Emergency Mitigation Service (EEMS) to automatically implement a URL rewrite rule aimed at blocking exploitation attempts. For air-gapped environments or systems where EEMS cannot be used, administrators can manually apply protections using the Exchange On-premises Mitigation Tool (EOMT). Microsoft has not yet revealed details about the threat actors involved in the attacks, the targeting scope, 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



Apply June 2026 Exchange Server Security Updates Immediately: Microsoft strongly advises organizations running Exchange Server to apply the June 2026 Security Updates for their respective Exchange Server versions without delay. Installing these updates is the most effective way to mitigate the vulnerability and prevent potential exploitation. Administrators should prioritize patch deployment across all affected systems, verify that updates have been successfully applied, and continue monitoring their environments for suspicious activity or unauthorized access attempts.



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.



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.



Potential MITRE ATT&CK TTPs

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



Patch Link

<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

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com