Microsoft Exchange Server Vulnerability [Actively Exploited]

Severity Level: HIGH

Components Affected

- Microsoft Exchange Server 2016 – all currently supported cumulative updates (CU23)
- Microsoft Exchange Server 2019 – all currently supported cumulative updates (CU14 and CU15)
- Microsoft Exchange Server Subscription Edition (SE) – RTM

Note: Exchange Online (Microsoft 365 hosted email) is not affected by this vulnerability.

Overview

A high-severity and actively exploited vulnerability (CVE – 2026 -42897) has been identified at on-premises Microsoft Exchange Server. This can be exploited by sending a specially crafted email, a remote attacker could cause arbitrary JavaScript to run in a victim's browser session when the message is opened or previewed in Outlook Web Access (OWA). This can lead to email spoofing, session token theft, mailbox impersonation and even the manipulation of the mailbox rules.

Description

Multiple vulnerabilities have been discovered in Exchange Server, the most severe of which could allow for cross-site scripting [XSS] and spoofing. The attacker does not require any access to the server as just a specifically crafted email delivered through the normal email pipeline and meeting certain user interactions can execute JavaScript inside the browser session. This gives the attacker a route to steal the session tokens, impersonate the mailbox server and even abuse the mailbox rules.

Impact

- Cross-Site Scripting [XSS]
- Mailbox Impersonation
- Spoofing
- Information Disclosure
- Session Hijacking / Token Theft

Solution/ Workarounds

Before applying for changes, please visit the vendor website for full details. Apply the vendor mitigations immediately and install the security update for affected Exchange Server versions as it becomes available through the June 2026 update cycle.

Recommended actions:

- Ensure the Exchange Emergency Mitigation (EM) Service is enabled. Microsoft has published an automatic mitigation (ID M2.1.x) for Exchange Server 2016, 2019, and SE, which is on by default. Verify it is applied using the Exchange Health Checker script.
- If the EM Service cannot be used (for example, on air-gapped servers), download the latest Exchange On-premises Mitigation Tool (EOMT) and apply the mitigation for CVE-2026-42897 via an elevated Exchange Management Shell.
- Install the security update for affected versions when available. The Exchange SE update is a publicly available security update; Exchange Server 2016 and 2019 updates are delivered to customers enrolled in the Period 2 Extended Security Update (ESU) program.
- Restrict or avoid accessing OWA through Internet Explorer or Microsoft Edge in Internet Explorer mode, as the mitigation does not protect those clients.
- Monitor mailboxes for suspicious inbox/transport rules, unusual OWA sessions, and indicators of session-token.

Vendor resources:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897
- https://techcommunity.microsoft.com/blog/exchange/addressing-exchange-server-may-2026-vulnerability-cve-2026-42897/4518498

Reference

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-42897
- https://nvd.nist.gov/vuln/detail/CVE-2026-42897

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.