GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 May 2026

Advisory 141: Microsoft Exchange Server Cross-Site Scripting Vulnerability

Release Date: 15th May 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-42897 is a high-severity reflected Cross-Site Scripting (XSS) vulnerability affecting the Outlook on the web (OWA) component of Microsoft Exchange Server. The flaw stems from improper neutralization of user-supplied input during web page generation. Discovered as a zero-day and actively exploited in the wild, the vulnerability allows unauthenticated attackers to execute arbitrary JavaScript within the security context of a targeted user's session, facilitating session hijacking and identity spoofing.

Microsoft confirms it had detected active exploitation of this vulnerability in the wild.

What are the systems affected?

The vulnerability affects on-premises versions of Microsoft Server:

- Exchange Server 2016
- Exchange Server 2019
- Exchange Server Subscription Edition (SE)

Exchange Server zero-days are particularly dangerous because they sit at the centre of corporate email, one of the most sensitive and widely used systems in any organisation.

What does this mean?

The attack is simple, effective, and requires minimal technical skill from the attacker's perspective:

Step 1 - Crafted Email Delivery - An attacker exploits this issue by sending a specially crafted email to a user. The email contains a malicious payload embedded in its content or a specially constructed URL targeting OWA parameters.

Step 2 - Victim Opens in OWA - The exploit path does not begin with a server takeover. Instead, the attacker sends a crafted email that leads to arbitrary JavaScript execution in the victim's browser session when viewed through OWA, creating a route to spoofing and session abuse in the web client context.

Step 3 - JavaScript Executes in Browser - The OWA server reflects the attacker's payload back in the HTTP response without sanitisation, resulting in arbitrary JavaScript execution within the security context of the victim's authenticated session.

Step 4 - Session Hijacking and Account Takeover - By capturing the session token, the attacker assumes the identity of the authenticated user. This allows the attacker to interact with the OWA interface directly, bypassing primary authentication mechanisms such as Multi-Factor Authentication (MFA), provided the session token remains valid.

Step 5 - Mailbox Compromise and Lateral Movement Once the session is hijacked, the attacker gains access to the victim's mailbox. The attacker can read sensitive correspondence, exfiltrate file attachments, and send emails on behalf of the compromised user. This facilitates lateral movement within the organisation, as the attacker can leverage the trusted internal account to launch further phishing campaigns or distribute malware to internal employees.

Mitigation process

CERTVU recommends the following:

- Apply Microsoft security updates for the affected product

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-42897
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

.