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 RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

1 June 2026

Avis 141 : Vulnérabilité de type Cross-Site Scripting dans Microsoft Exchange Server

Date de publication : 15 mai 2026
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publie l'avis suivant.

Cette alerte s'adresse aux organisations ainsi qu'aux administrateurs de systèmes et réseaux utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et des administrateurs de systèmes.

Objet de l'alerte

CVE-2026-42897 est une vulnérabilité de type Cross-Site Scripting (XSS) réfléchi, classée de sévérité élevée, affectant le composant Outlook Web Access (OWA) de Microsoft Exchange Server. Cette vulnérabilité résulte d'une neutralisation inadéquate des données fournies par l'utilisateur lors de la génération des pages web. Identifiée comme une vulnérabilité zero-day et activement exploitée dans des environnements réels, elle permet à des attaquants non authentifiés d'exécuter du code JavaScript arbitraire dans le contexte de sécurité de la session d'un utilisateur ciblé. Cette exploitation peut entraîner notamment le détournement de session et l'usurpation d'identité.

Microsoft a confirmé avoir détecté une exploitation active de cette vulnérabilité dans la nature.

Systèmes concernés

La vulnérabilité affecte les versions sur site de Microsoft Server :

- Exchange Server 2016
- Exchange Server 2019
- Exchange Server Édition par Abonnement (SE)

Les failles zero-day dans Exchange Server sont particulièrement dangereuses, car elles se trouvent au cœur de la messagerie d'entreprise, l'un des systèmes les plus sensibles et les plus utilisés dans toute organisation.

Implications

L'attaque est simple, efficace et nécessite peu de compétences techniques du point de vue de l'attaquant.

Étape 1 - Livraison d'un courriel spécialement conçu - Un attaquant exploite cette vulnérabilité en envoyant à un utilisateur un courriel forgé. Le message contient soit une charge utile malveillante intégrée dans son contenu, soit une URL construite de manière spécifique visant les paramètres OWA.

Étape 2 - Ouverture par la victime dans OWA - L'exploitation ne débute pas par une compromission du serveur. L'attaquant transmet un courriel spécialement conçu qui, lorsqu'il est ouvert via OWA, entraîne l'exécution de code JavaScript arbitraire dans la session du navigateur de la victime. Cette action ouvre la voie à l'usurpation d'identité et à l'abus de session dans le contexte du client web.

Étape 3 - Exécution du JavaScript dans le navigateur : Le serveur OWA renvoie la charge utile de l'attaquant dans la réponse HTTP sans procéder à une neutralisation adéquate. Cette faille entraîne l'exécution de code JavaScript arbitraire dans le contexte de sécurité de la session authentifiée de la victime.

Étape 4 - Détournement de session et prise de contrôle du compte : En capturant le jeton de session, l'attaquant usurpe l'identité de l'utilisateur authentifié. Il peut alors interagir directement avec l'interface OWA, contournant les mécanismes d'authentification primaire tels que l'authentification multifacteur (MFA), tant que le jeton de session demeure valide.

Étape 5 - Compromission de la boîte aux lettres et mouvement latéral : Une fois la session détournée, l'attaquant obtient un accès complet à la boîte aux lettres de la victime. Il peut consulter des correspondances sensibles, exfiltrer des pièces jointes et envoyer des courriels au nom de l'utilisateur compromis. Cette situation facilite le mouvement latéral au sein de l'organisation, car l'attaquant peut exploiter le compte interne de confiance pour lancer de nouvelles campagnes d'hameçonnage ou diffuser des logiciels malveillants auprès des employés internes.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

- Appliquer les mises à jour de sécurité Microsoft pour le produit concerné.

Références

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

.