DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 16-05-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Microsoft Exchange Server
Réference	1471
Date de Publication	2026-05-15
Sévérité	Critique

IMPACT :

- Usurpation d'identité (Spoofing)
- Exécution de code JavaScript arbitraire dans le navigateur de la victime

SYSTÉME AFFECTÉ :

- Microsoft Exchange Server 2016,
- Microsoft Exchange Server 2019
- Exchange Server Subscription Edition (toutes les mises à jour).
- Les déploiements Microsoft Exchange Online (cloud) ne sont pas affectés.

DÉSCRIPTION :

Une vulnérabilité critique a été découverte dans Exchange Server. Cette faille, activement exploitée dans la nature, affecte le service Outlook Web Access (OWA) des serveurs Exchange on-premises. Un attaquant non authentifié peut l'exploiter en envoyant un courriel spécialement conçu à un utilisateur ciblé. Si le destinataire ouvre le message malveillant dans Outlook Web Access, du code JavaScript arbitraire s'exécute dans son navigateur, permettant le détournement de session ou la manipulation des données locales du navigateur.

CONTOURNEMENT PROVISOIRE :

Aucun correctif définitif n’est encore disponible. Microsoft a publié une mesure d’atténuation temporaire :

1. Vérifier que le service **Exchange Emergency Mitigation Service (EEMS)** est activé pour appliquer automatiquement la mitigation **M2.1.x**.

2. Pour les environnements déconnectés ou air-gapped, télécharger et exécuter manuellement la dernière version du **Exchange On-premises Mitigation Tool** via un shell d’administration avec privilèges élevés.

3. Maintenir la mitigation active malgré les effets secondaires mineurs (fonction d’impression de calendrier OWA et affichage des images en ligne perturbés).

4. Mettre à jour les versions anciennes (Exchange 2016/2019) vers une version supportée par le programme **Extended Security Update (Period 2)** afin de pouvoir recevoir le correctif définitif lors de sa publication.

5. Sensibiliser les utilisateurs à la vigilance face aux courriels suspects et envisager temporairement l’utilisation du client Outlook Desktop à la place d’OWA.

DOCUMENTATION :

CVE-2026-42897 :

- https://www.cve.org/CVERecord?id=CVE-2026-42897