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

28 April 2026

Avis 132 : Vulnérabilité de désérialisation de données non fiables dans Microsoft Exchange Server (CVE-2023-21529)

Date de publication : 13 avril 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-2023-21529 est une vulnérabilité de haute gravité permettant l'exécution de code à distance (RCE) et affectant Microsoft Exchange Server. La faille est causée par la désérialisation de données non fiables (CWE-502), lorsque l'application traite de manière incorrecte des objets sérialisés.

Lorsque Exchange Server désérialise des données contrôlées par un attaquant sans validation appropriée, il peut exécuter des charges utiles malveillantes intégrées dans ces données, entraînant l'exécution de code arbitraire sur le serveur.

Systèmes concernés

Versions affectées :

- Exchange Server 2013 (CU23)

- Exchange Server 2016 (CU23)
- Exchange Server 2019 (CU11 et CU12)

Exchange Server est largement utilisé pour :

- Systèmes de messagerie d'entreprise ;
- Infrastructures de communication et de messagerie ;
- Services de collaboration et de communication.

En raison de son exposition fréquente à Internet et de son rôle critique dans les opérations des organisations, Exchange Server constitue une cible privilégiée et de grande valeur pour les attaquants.

Implications

L'exploitation nécessite un **accès authentifié**, mais les privilèges requis peuvent être faibles.

Chaîne d'exploitation typique :

1. **Accès initial**
   - L'attaquant obtient des identifiants valides (par exemple via du phishing, un vol d'identifiants ou une compromission préalable).
2. **Création d'une charge utile sérialisée malveillante**
   - L'attaquant conçoit un objet spécialement conçu pour exploiter la logique de désérialisation d'Exchange Server.
3. **Envoi de la charge utile**
   - La charge est transmise à un point de terminaison vulnérable d'Exchange Server via des requêtes réseau.
4. **Désérialisation non sécurisée**
   - Exchange Server traite (désérialise) l'objet malveillant sans validation adéquate.
5. **Exécution de code à distance**
   - La charge exécute des commandes arbitraires sur le serveur avec les privilèges du service Exchange (souvent au niveau SYSTEM).

L'exploitation réussie de cette vulnérabilité peut permettre aux attaquants de :

- Exécuter du code arbitraire sur le serveur Exchange.
- Prendre le contrôle complet du système.
- Accéder à ou exfiltrer des données sensibles de messagerie.
- Modifier ou supprimer des boîtes aux lettres et des configurations.
- Se déplacer latéralement au sein du réseau de l'entreprise.
- Déployer des logiciels malveillants ou des rançongiciels.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

1. Appliquer les mises à jour de sécurité Microsoft (critique)

- Installer immédiatement les dernières mises à jour de sécurité d'Exchange Server (par exemple KB5023038 et ultérieures).

2. Restreindre l'accès et renforcer l'authentification

- Mettre en place l'authentification multi facteur (MFA).
- Limiter l'accès aux services Exchange aux réseaux de confiance.
- Surveiller et restreindre les comptes disposant de privilèges élevés.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2023-21529
3. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21529

.