aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans OwnCloud

2023-11-27 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-49103

Le 21 novembre 2023, OwnCloud a publié un bulletin de sécurité indiquant la découverte d'une nouvelle vulnérabilité critique (CVE-2023-49103) dans leur solution.

Deux autres vulnérabilités critiques sont listées dans le bulletin de sécurité : CVE-2023-49104 et CVE-2023-49105.

OwnCloud est une solution open-source permettant de mettre en place son propre serveur de stockage, de partage et de synchronisation de fichiers.

La faille affecte l'application *graphapi* qui s'appuie sur une bibliothèque tierce pour générer une URL.

En accédant à cette url, l'attaquant peut récupérer des informations de configuration de l'environnement PHP (phpinfo), comme le mot de passe administrateur et des identifiants d'un serveur de messagerie configuré dans ownCloud.

Si cette vulnérabilité ne semble pas être encore exploitée, une preuve de concept (POC) est disponible. Près de 2000 serveurs exposés sur internet et localisés en France, disposent d'un service ownCloud.

Type de vulnérabilité

- **CWE-200** : Exposure of Sensitive Information to an Unauthorized Actor

Risques

- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- Bibliothèque OwnCloud graphapi versions 0.2.x
- Bibliothèque OwnCloud graphapi versions 0.3.x
- Les conteneurs Docker antérieurs à février 2023 ne sont pas vulnérables à la divulgation des informations d'identification.

Recommandations

L'éditeur recommande de supprimer le fichier *GetPhpInfo* présent dans owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/.

Des informations complémentaires sont disponibles dans le bulletin de l'éditeur.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Références

- https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0970/