aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Roundcube

2024-02-13 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-43770

Le 18 septembre 2023, Roundcube a publié un bulletin de sécurité concernant une vulnérabilité dans son produit *Roundcube Webmail*.

Cette faille, découverte par le chercheur en sécurité Niraj Shivtarkar, est due à un défaut de traitement des *linkrefs* dans le fichier *program/lib/Roundcube/rcube_string_replacer.php*. Elle permet à un attaquant distant et non authentifié d'injecter du code indirect (XSS) interprété par le serveur mail.

Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 12 février 2024.

Type de vulnérabilité

- CWE-79 : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Risque

- Injection de code indirecte (XSS)

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Roundcube Webmail versions comprises entre 1.4.0 et 1.4.13
- Roundcube Webmail versions comprises entre 1.5.0 et 1.5.3
- Roundcube Webmail versions comprises entre 1.6.0 et 1.6.2

Recommandations

- Mettre à jour Roundcube Webmail vers la version 1.4.14, 1.5.4, 1.6.3 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Roundcube.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Références

- https://www.cve.org/CVERecord?id=CVE-2023-43770
- https://roundcube.net/news/2023/09/18/security-update-1.4.14-released
- https://roundcube.net/news/2023/09/18/security-update-1.5.4-released
- https://roundcube.net/news/2023/09/15/security-update-1.6.3-released
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0786/
- https://www.cisa.gov/news-events/alerts/2024/02/12/cisa-adds-one-known-exploited-vulnerability-catalog