aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans PRIM’X

2023-12-14 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

PRIM'X

L'éditeur de logiciels de chiffrement d'infrastructures, *Prim'x*, annonce le 13 décembre 2023 la mise à disposition de correctifs concernant six vulnérabilités :

- CVE-2023-50439 score 5.3
- CVE-2023-50440 score 7.5
- CVE-2023-50441 score 4.8
- CVE-2023-50442 score 4.1
- CVE-2023-50443 score 4.0
- CVE-2023-50444 score 8.7

Ce bulletin aborde la vulnérabilité, CVE-2023-50444, affectant le produit *ZED! Entreprise* (Windows).

ZED - CVE-2023-50444

Des chercheurs en sécurité ont découvert que les métadonnées du conteneur .ZED sont vulnérables à une attaque par force brute, lorsque le mot de passe de l'utilisateur est faible.

L'exploitation de cette faille par un attaquant distant et non authentifié permet de divulguer des informations sensibles de l'utilisateur.

Types de vulnérabilités

- **CWE-200** : Exposure of Sensitive Information to an Unauthorized Actor
- **CWE-284** : Improper Access Control
- **CWE-266** : Incorrect Privilege Assignment

Risque

- Divulgation d'information

Criticité (score de base CVSS v3.1)

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

Produits impactés

- *ZED! Entreprise* (Windows), les versions antérieures à 2023.5. Inclus les versions Q.2020.1, Q.2020.2 et Q.2021.1.
- *ZED!* fonctionnalités de *ZONECENTRAL* (Windows), les versions antérieures à 2023.5, y compris la version Q.2021.1
- *ZED!* fonctionnalités de *ZEDMAIL* (Windows), les versions antérieures à 2023.5.

Recommandations

Les correctifs

- *ZED! Entreprise* (Windows), mettre à jour vers la version Q.2020.3 (version validée par l'ANSSI) ;
- *ZED! Entreprise* (Windows), mettre à jour vers la version Q.2021.2 (version validée par l'ANSSI) ;
- *ZED! Entreprise* (Windows), mettre à jour vers la version minimale 2023.5 ;
- *ZED!* fonctionnalités de *ZONECENTRAL* (Windows), mettre à jour vers la version Q.2021.2 (version validée par l'ANSSI) ;
- *ZED!* fonctionnalités de *ZONECENTRAL* (Windows), mettre à jour vers la version minimale 2023.5 ;
- *ZED!* fonctionnalités de *ZEDMAIL* (Windows), mettre à jour vers la version minimale 2023.5 ;

Site de l'éditeur

- Des informations complémentaires sont disponibles sur le site de l'éditeur.

Recommandations spécifiques de l'ANSSI

En complément du déploiement des correctifs, il est nécessaire de :

- Créer de nouveaux conteneurs Zed! et ne pas réutiliser les anciens ;
- Appliquer une politique de mot de passe forte pour les mots de passe utilisateurs (si la liste d'accès est protégée par mot de passe). La lecture de la documentation suivante est recommandée Recommandations relatives à l'authentification multifacteur et aux mots de passe ;
- Contrôler les droits d'accès aux fichiers de zone utilisés par ZoneCentral enfin d'en limiter les droits d'écriture aux seuls administrateurs ZoneCentral.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en source ouverte.

Références

CVE-2023-50444

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-1021/
- https://nvd.nist.gov/vuln/detail/CVE-2023-50444
- https://www.primx.eu/en/bulletins/security-bulletin-23B30874/

PRIM'X

- https://www.primx.eu/en/bulletins/security-bulletin-23b30930/
- https://www.primx.eu/en/bulletins/security-bulletin-23b3093b/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30874/
- https://www.primx.eu/en/bulletins/security-bulletin-23b3093a/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30931/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30933/

ANSSI

- https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe