ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	« Supply chain attaque » Compromission du package PyPI elementary-data
Numéro de Référence	63602804/26
Date de Publication	28 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Package PyPI : elementary-data==0.23.3 (version compromise)

Bilan de la vulnérabilité

En avril 2026, des chercheurs en sécurité ont identifié une compromission du package Python « elementary-data », une bibliothèque utilisée dans les environnements de data engineering et de data quality, avec environ 11 millions de téléchargements mensuels.

Cette attaque de chaîne d'approvisionnement résulte de la publication d'une version malveillante (0.23.3) sur le dépôt PyPI. Cette version contient un infostealer permettant l'exfiltration de données sensibles depuis les environnements des développeurs et systèmes CI/CD.

Une version corrigée a été publiée pour remplacer la version compromise.

Toute machine ayant installé ou exécuté la version 0.23.3 doit être considérée comme potentiellement compromise.

Le code injecté:

- S'exécute automatiquement lors de l'installation du package (pip install) ;
- Collecte des informations sensibles (tokens, clés API, variables d'environnement) ;
- Exfiltre les données vers une infrastructure distante contrôlée par l'attaquant ;
- Peut compromettre des environnements CI/CD, cloud et postes développeurs ;

Solution

1. Vérifiez si la version suivante est utilisée :
    - elementary-data==0.23.3
2. Si oui:

- Isoler immédiatement la machine ou le serveur concerné ;
- Désinstaller le package compromis ;
- Supprimer et reconstruire les environnements Python (virtualenv, Docker, etc.) ;
- Installer une version saine (dernière version non compromise disponible sur PyPI) ;
- Ne pas se limiter à un simple upgrade sans audit ;
- Régénérer tous les secrets potentiellement exposés (tokens API, clés SSH, accès cloud, etc.) ;
- Analyser les logs pour détecter toute exfiltration ;
- Surveiller les connexions réseau sortantes suspectes ;

Risque

- Exfiltration de données sensibles
- Compromission des environnements de développement
- Vol de secrets cloud et API keys
- Compromission de chaînes CI/CD
- Exécution de code arbitraire

Annexe

Bulletins de sécurité :

- https://www.bleepingcomputer.com/news/security/pypi-package-with-11m-monthly-downloads-hacked-to-push-infostealer/
- https://pypi.org/project/elementary-data/0.23.4/