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 npm axios
Numéro de Référence	62680104/26
Date de Publication	01 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- npm axios@1.14.1
- npm axios@0.30.4
- Dépendance malveillante : plain-crypto-js@4.2.1

Bilan de la vulnérabilité

Le 31 mars 2026, des chercheurs en sécurité ont détecté une compromission du package « npm axios », l'un des clients HTTP JavaScript les plus utilisés (plus de 100 millions de téléchargements hebdomadaires). Cette attaque de chaîne d'approvisionnement résulte de la compromission du compte npm du mainteneur du package axios. Les attaquants ont publié des versions malveillantes intégrant un cheval de Troie d'accès à distance (RAT). Toute machine ayant installé une des versions susmentionnées doit être considérée comme totalement compromise.

Le code injecté:

- Télécharge et exécute un payload spécifique à l'OS (Windows, Linux, macOS) ;
- Établit une communication avec un serveur de commande et contrôle (C2) ;
- Exfiltre des informations sensibles (tokens, clés API, credentials) ;
- Permet l'exécution de commandes à distance et le contrôle complet du système ;
- Supprime ses traces après exécution pour éviter la détection ;

Solution

1. Vérifiez si l'un des packages suivants est installé dans vos projets :
    - axios@1.14.1
    - axios@0.30.4
    - plain-crypto-js@4.2.1

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

2. Si oui:
    - Isoler immédiatement la machine ou le serveur concerné ;
    - Supprimer complètement les environnements compromis (rebuild recommandé) ;
    - Ne pas se contenter d'un simple downgrade ;
    - Supprimer le dossier node_modules/plain-crypto-js ;
    - Installer une version sûre :
        - axios@1.14.0 (branche 1.x)
        - axios@0.30.3 (branche 0.x)
    - Audit de sécurité recommandé pour les projets ayant indirectement utilisé ce package (via des dépendances) ;
    - Régénérer tous les secrets (tokens npm, clés API, accès cloud, SSH, etc.) ;
    - Surveiller les connexions réseau suspectes.

Indicateurs de compromission (IOCs):

Hash:

- 2553649f2322049666871cea80a5d0d6adc700ca
- d6f3f62fd3b9f5432f5782b62d8cfd5247d5ee71
- 07d889e2dadce6f3910dcbc253317d28ca61c766

Packages npm malveillants:

- axios@1.14.1
- axios@0.30.4
- plain-crypto-js@4.2.1

Fichiers et chemins suspects:

- /Library/Caches/com.apple.act.mond
- %PROGRAMDATA%\wt.exe
- %TEMP%\6202033.vbs
- %TEMP%\6202033.ps1
- /tmp/ld.py

Infrastructure réseau (C2):

- sfrclak[.]com
- 142.11.206[.]73

- http://sfrclak[.]com:8000/6202033

Risque

- Exécution de code à distance (RCE)
- Exfiltration de données sensibles
- Installation persistante d'un cheval de Troie (RAT)

Annexe

Bulletins de sécurité :

- https://www.aikido.dev/blog/axios-npm-compromised-maintainer-hijacked-rat
- https://socket.dev/blog/axios-npm-package-compromised