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	Compromission de la chaîne d'approvisionnement du package npm Cline
Numéro de Référence	61342302/26
Date de Publication	23 Février 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Cline CLI (via npm) version antérieure à 2.4.0 ;

Identificateurs externes

- GHSA-9ppg-jx86-fqw7;

Bilan de la vulnérabilité

Une compromission de la chaîne d'approvisionnement (Supply Chain Attack) a été corrigée dans l'outil « Cline CLI ». Un attaquant a utilisé un jeton de publication compromis pour injecter un script "postinstall" non autorisé. L'installation de la version infectée entraîne l'installation automatique et globale du package tiers « openclaw » sur le système de l'utilisateur.

Les utilisateurs ayant installé ou mis à jour Cline en ligne de commande le 17 février 2026 (entre 11h26 et 19h30 GMT environ) ont probablement installé le package tiers openclaw de manière automatisée et non sollicitée sur leur système.

Solution :

Veuillez mettre à jour Cline CLI vers la version v2.4.0 ou supérieure via la commande « npm install -g cline@latest ». Il est également recommandé de désinstaller manuellement le package non sollicité avec « npm uninstall -g openclaw ».

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

Risque :

- Exécution de code non autorisé ;
- Porter atteinte à la confidentialité des données ;

Annexe

Bulletin de sécurité Cline**:**

- https://github.com/cline/cline/security/advisories/GHSA-9ppg-jx86-fqw7