**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**

**NOTE DE SECURITE**

| | |
|---|---|
| **Titre** | « Supply chain attaque » Compromission de plusieurs packages npm |
| **Numéro de Référence** | 56610909/25 |
| **Date de Publication** | 09 Septembre 2025 |
| **Risque** | Critique |
| **Impact** | Critique |

Le 08 Septembre 2025, une attaque de chaîne d'approvisionnement logicielle a compromis plusieurs packages populaires de l'écosystème « npm », suite au piratage du compte du responsable des packages, ciblé par une campagne de phishing. L'attaquant a obtenu les identifiants, mot de passe et jeton 2FA via une attaque de type Adversary-in-the-Middle (AitM), lui permettant de publier des versions malveillantes de 20 packages largement utilisés, représentant ensemble plus de 2 milliards de téléchargements hebdomadaires.

Le code injecté agit comme un intercepteur de transactions dans les navigateurs, en surveillant et en modifiant les appels effectués via (window.fetch, XMLHttpRequest ou encore window.ethereum.request). Ce mécanisme détourne les adresses de portefeuilles numériques pour rediriger les fonds vers ceux de l'attaquant. L'attaque cible principalement les utilisateurs finaux connectant un portefeuille crypto à une application intégrant un package compromis.

Les applications intégrant ces dépendances compromises peuvent devenir des vecteurs d'intrusion, permettant l'installation des backdoors, le vol de clés API ou l'exfiltration de données sensibles. Il est donc vivement recommandé aux utilisateurs de mettre à jour toute solution reposant sur les versions vulnérables des packages, d'auditer leurs pipelines et de renforcer la surveillance afin de détecter tout comportement anormal dans les environnements concernés.

## Indicateurs de compromission (IOCs):

Packages npm malveillants:

- ansi-regex@6.2.1
- ansi-styles@6.2.2

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

- backslash@0.2.1
- chalk@5.6.1
- chalk-template@1.1.1
- color-convert@3.1.1
- color-name@2.0.1
- color-string@2.1.1
- debug@4.4.2
- error-ex@1.3.3
- has-ansi@6.0.1
- is-arrayish@0.3.3
- proto-tinker-wc@1.8.7
- supports-hyperlinks@4.1.1
- simple-swizzle@0.2.3
- slice-ansi@7.1.1
- strip-ansi@7.1.1
- supports-color@10.2.1
- wrap-ansi@9.0.1

Fichiers et chemins suspects:

- Injection de JavaScript malveillant dans les packages.

  Le code intercepte :

✓ window.fetch

✓ XMLHttpRequest

✓ window.ethereum.request

## Annexe

- https://bsky.app/profile/bad-at-computer.bsky.social/post/3lydioq5swk2y
- https://thehackernews.com/2025/09/20-popular-npm-packages-with-2-billion.html