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
Numéro de Référence	54351205/25
Date de Publication	12 Mai 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- npm rand-user-agent@1.0.110
- npm rand-user-agent@2.0.83
- npm rand-user-agent@2.0.84

Bilan de la vulnérabilité

Le 5 mai 2025, des chercheurs en sécurité ont détecté une compromission des versions 2.0.83, 2.0.84 et 1.0.110 du package « npm `rand-user-agent` » dans une attaque de chaîne d'approvisionnement. Ce package est utilisé pour générer des user-agents aléatoires dans les contextes de scraping ou de tests automatisés.

Le code injecté:

- Crée un répertoire caché « ~/.node_modules »
- Altère les chemins de modules pour y charger axios et socket.io-client
- Établit une connexion persistante avec un serveur C2 (http://85.239.62.36:3306)
- Exfiltre des informations système (hostname, OS, UUID, etc.)
- Active un RAT (Remote Access Trojan) capable d'exécuter des commandes à distance, d'exfiltrer des fichiers, et de contrôler le système infecté

Solution

1. Vérifiez si l'un des packages suivants est installé dans vos projets :
    - rand-user-agent@2.0.83
    - rand-user-agent@2.0.84
    - rand-user-agent@1.0.110
2. Si oui:
    - Isoler immédiatement la machine ou le serveur concerné

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

- Effectuer un scan complet du système (recherchez `~/.node_modules`, connexions réseau suspectes, processus persistants)
- Supprimer les versions malveillantes et leurs effets (le simple downgrade ne suffit pas)
- Regénérer toutes les clés et jetons d'accès susceptibles d'avoir été exposés
- Mettre à jour vers la dernière version sûre (>=2.0.82)
- Audit de sécurité recommandé pour les projets ayant indirectement utilisé ce package (via des dépendances).

Indicateurs de compromission (IOCs):

IPs:

- 85.239.62.36 (port 3306)

Packages npm malveillants:

- rand-user-agent@1.0.110
- rand-user-agent@2.0.83
- rand-user-agent@2.0.84

Fichiers et chemins suspects:

- ~/.node_modules/ (répertoire caché créé pour charger des dépendances malicieuses)
- dist/index.js (contenant du code obfusqué dans les versions compromises)

Risque

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

Annexe

Bulletin de sécurité :

- https://www.aikido.dev/blog/catching-a-rat-remote-access-trojian-rand-user-agent-supply-chain-compromise
- https://www.bleepingcomputer.com/news/security/supply-chain-attack-hits-npm-package-with-45-000-weekly-downloads/