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 » des packages npm officiels de SAP
Numéro de Référence	63713004/26
Date de Publication	30 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

SAP CAP (Cloud Application Programming Model) MTA Packages :

- mbt@1.2.48
- @cap-js/db-service@2.10.1
- @cap-js/postgres@2.2.2
- @cap-js/sqlite@2.2.2

Bilan de la vulnérabilité

Le 29 avril 2026, des chercheurs en sécurité (Aikido, Socket, Wiz) ont détecté une compromission de plusieurs packages « npm » officiels de SAP, utilisés pour le développement d'applications cloud (CAP) et la gestion d'archives multi-cibles (MTA). Cette attaque de chaîne d'approvisionnement, baptisée "mini Shai-Hulud", est attribuée au groupe "TeamPCP". Les attaquants ont injecté un script malveillant de type "preinstall" qui s'exécute automatiquement lors de l'installation du package. L'objectif principal est le vol massif des identifiants de développeurs et de secrets d'environnements CI/CD.

Cette attaque présente un niveau de sophistication élevé et un fort potentiel de diffusion au sein des environnements compromis. En conséquence, toute installation ou utilisation des versions affectées doit être considérée comme un incident de sécurité critique nécessitant une réponse immédiate.

Le code injecté:

- Exécute un script « setup.mjs » qui télécharge le runtime JavaScript « Bun » depuis GitHub pour exécuter le payload ;
- Déploie un payload (execution.js) obfusqué conçu pour l'exfiltration des données ;
- Cible spécifiquement les secrets CI/CD en lisant directement la mémoire des processus (/proc/<pid>/mem);

- Collecte des tokens npm, GitHub, des clés SSH, ainsi que des accès cloud (AWS, Azure, GCP) et des configurations Kubernetes ;
- Extrait les mots de passe stockés dans les navigateurs (Chrome, Safari, Edge, Brave) ;
- Exfiltre les données vers des dépôts GitHub publics créés sur le compte de la victime avec la description "A Mini Shai-Hulud has Appeared".

Solution

- Isoler les machines de développement et suspendre les pipelines CI/CD concernés ;
- Supprimer les versions compromises et forcer une version saine;
- Régénérer tous les secrets potentiellement exposés : tokens GitHub/npm, clés d'accès Cloud (AWS/Azure/GCP), certificats SSH et accès Kubernetes ;
- Réinitialiser les mots de passe des navigateurs si le développeur travaillait sur une machine infectée ;
- Inspecter les dépôts GitHub pour détecter la création de nouveaux dépôts suspects ou l'injection de workflows malveillants.

Indicateurs de compromission (IOCs):

Hash:

- setup.mjs: 4066781fa830224c8bbcc3aa005a396657f9c8f9016f9a64ad44a9d7f5f45e34
- execution.js: 6f933d00b7d05678eb43c90963a80b8947c4ae6830182f89df31da9f568fea95
- embedded GitHub runner memory dumper: 29ac906c8bd801dfe1cb39596197df49f80fff2270b3e7fbab52278c24e4f1a7

Packages npm malveillants:

- @cap-js/sqlite - v2.2.2
- @cap-js/postgres - v2.2.2
- @cap-js/db-service - v2.10.1
- mbt@1.2.48

Chaînes de caractères suspectes:

- A Mini Shai-Hulud has Appeared
- OhNoWhatsGoingOnWithGitHub (propagation keyword / GitHub commit dead-drop marker)
- ctf-scramble-v2
- tmp.987654321.lock
- chore: update dependencies

- claude@users.noreply.github.com

Infrastructure réseau (C2):

- hxxps://github[.]com/oven-sh/bun/releases/download/bun-v1.3.13/
- hxxps://api.github[.]com/search/commits?q=OhNoWhatsGoingOnWithGitHub&sort=author-date&order=desc&per_page=50
- hxxp://169.254.169.254
- hxxp://169.254.170.2
- hxxp://[fd00:ec2::254]

Risque

- Exfiltration de données sensibles
- Compromission des environnements CI/CD
- Accès non autorisé aux infrastructures cloud
- Propagation via la chaîne d'approvisionnement
- Exécution de code arbitraire
- Compromission globale des systèmes et projets

Annexe

Bulletins de sécurité :

- https://www.bleepingcomputer.com/news/security/official-sap-npm-packages-compromised-to-steal-credentials/
- https://socket.dev/blog/sap-npm-packages-compromised-credential-stealer
- https://www.aikido.dev/blog/sap-npm-packages-hijacked-to-steal-cloud-credentials