GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

11 décembre 2025

Avis 113 : Faille dans la chaîne logistique de Shai Hulud 2.0

Date de publication : 24 novembre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

Shai Hulud 2.0 est un logiciel malveillant auto-propagateur ciblant l'écosystème NPM (Node Package Manager). Il se propage via des paquets NPM malveillants qui exécutent des scripts de cycle de vie afin de s'approprier les identifiants des développeurs et de compromettre GitHub, GitLab, Azure DevOps et les services cloud.

En savoir plus.

Systèmes concernés

- Machines de développement utilisant Node.js, NPM, NVM.
- Pipelines CI/CD (GitHub Actions, GitLab CI, Azure DevOps).
- Environnements de développement basés sur Docker, WSL et VM.
- Comptes cloud (AWS, Azure, GCP) via des clés API et des jetons divulgués.

Implication

Les attaquants peuvent exploiter cette vulnérabilité par les manières suivantes (vecteur d'attaque).

Les attaquants publient des paquets NPM malveillants contenant un script d'installation caché qui :

- Récupère les jetons API Keys, les variables d'environnement et les clés SSH.
- Télécharge les données volées sur GitHub à l'aide du compte de la victime.
- Crée de nouveaux référentiels pour diffuser les paquets infectés.
- Permet une réinfection via les mises à jour de dépendances et l'automatisation CI/CD.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

- Isolez les systèmes affectés du réseau pour empêcher la propagation.
- Remplacez toutes les informations d'identification stockées sur les machines des développeurs ou dans les environnements CI/CD (GitHub/GitLab/Azure DevOps, clés API Cloud, clés SSH, fichiers.env).
- Vérifiez les référentiels et les journaux CI/CD pour détecter les commits et les activités non autorisés.
- Désactivez le script de cycle de vie NPM.

Références

1. https://about.gitlab.com/blog/gitlab-discovers-widespread-npm-supply-chain-attack/
2. https://www.zscaler.com/blogs/security-research/shai-hulud-v2-poses-risk-npm-supply-chain