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 REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

11 December 2025

Advisory 113: Shai Hulud 2.0 Supply Chain Compromise

Release Date: 24th of November 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

Shai Hulud 2.0 is a self-propagating supply chain Malware targeting the NPM (Node Package Manager) ecosystem. It spreads through malicious NPM packages that execute lifecycle scripts to steal developer credentials and compromise Git-Hub, Git-Lab, Azure DevOps, and cloud services.

Read more.

What are the Systems affected?

- Developer machines using Node.js, NPM, NVM
- CI/CD pipelines (GitHub Actions, GitLab CI, Azure DevOps)
- Docker, WSL, and VM-based development environments
- Cloud accounts (AWS, Azure, GCP) via leaked API keys and tokens

What does this mean?

How attackers exploit this vulnerability (attack vector)

Attackers publish malicious NPM packages containing hidden install script that:

- Harvest tokens API Keys, environment variables, SSH keys
- Upload stolen data to GitHub using the victim's account
- Create new repositories to spread infected packages
- Enable re-infected through dependency updates and CI/CD automation

Mitigation process

CERTVU recommend:

- Isolate affected systems from the network to stop propagation.
- Rotate all credentials stored on developer machines or CI/CD environments (GitHub/GitLab/Azure DevOps, Cloud API keys, SSH keys, .env files).
- Review repositories and CI/CD logs for unauthorised commits and activities.
- Disable NPM lifecycle script

Reference

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