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

12 Januari 2026

Advaes namba 113: Atak blong Saplae Jen blong *Shai Hulud 2.0*

Deit we hemi rilis: 24 Novemba 2025
Impak: HAE / KRITIKOL
TLP: KLIA

Dipatmen blong Komunikesen mo Dijitol Transfomesen (DKDT) tru long CERT Vanuatu (CERTVU), i givimaot advaeseri ia.

Woning ia hem i blong olgeta Oganaesesen mo Sistem/Netwok Administreta we oli yusum prodak ia. Woning ia oli mekem blong olgeta teknikol yusa mo sistem administreta oli andastanem.

Wanem ia?

Shai Hulud 2.0 hem i wan *self-propagating* saplae jen *Malware* we i stap tagetem NPM (Node Package Manager) ekosistem. Hem i spred tru long ol denjares NPM pakej we oli eksekutim ol laefsaekol skript blong stilim ol kredensol blong divelopa mo tekem kontrol long Git-Hub, Git-Lab, Azure DevOps, mo ol cloud seves.

Ridim moa long ples ia.

Hemia i afektem wanem Sistem?

- Ol divelopa masin we oli stap yusum Node.js, NPM, NVM
- Ol CI/CD paeplaen (GitHub Actions, GitLab CI, Azure DevOps)
- Docker, WSL, mo ol VM-bes divelopmen envaeromen
- Ol Cloud akaon (AWS, Azure, GCP) tru long ol API ki mo token we oli no moa haed

Hemia i minim wanem?

Olsem wanem ol ataka oli eksploitem vulnerabiliti ia (atak vekta)

Ol ataka oli pablisim ol denjares NPM pakej we i gat instol skript we i haed we i:

- Havestem ol token *API Keys*, ol envaeromen varaebol, ol SSH keys
- Aplodem ol data we oli stilim long GitHub tru long akaon blong viktim
- Krietem ol niu repositori blong spredem ol pakej we oli infekted
- Enebolem *re-infected* tru ol dipendensi apdeit mo CI/CD *automation*

Proses blong Katem Daon Risk

CERTVU i rikomendem se:

- Aesoletem ol sistem we oli afekted stat long netwok blong stopem transmisen.
- Rotetem evri kredensol we oli storem long ol on divelopa masin o ol CI/CD envaeromen (GitHub/GitLab/Azure DevOps, Cloud API keys, SSH keys, .env files).
- Riviuem ol repositori mo ol CI/CD log from ol komit mo aktiviti we oli no otoraesem.
- Disebolem NPM laefsaekol skript

Refrens

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