

Forum:[Hack Forums](#)

Thread: [Widespread Supply Chain Compromise Impacting npm Ecosystem](#)

Stanley - October 12, 2025, 6:35 am

Widespread Supply Chain Compromise Impacting npm Ecosystem

CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world's largest JavaScript registry, npmjs.com. A self-replicating worm—publicly known as “Shai-Hulud”—has compromised over 500 packages.[i]

After gaining initial access, the malicious cyber actor deployed malware that scanned the environment for sensitive credentials. The cyber actor then targeted GitHub Personal Access Tokens (PATs) and application programming interface (API) keys for cloud services, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.[ii]

The malware then:

- Exfiltrated the harvested credentials to an endpoint controlled by the actor.

- Uploaded the credentials to a public repository named Shai-Hulud via the GitHub/user/repos API.

- Leveraged an automated process to rapidly spread by authenticating to the npm registry as the compromised developer, injecting code into other packages, and publishing compromised versions to the registry.[iii]

CISA urges organizations to implement the following recommendations to detect and remediate this compromise:

- Conduct a dependency review of all software leveraging the npm package ecosystem.

- Check for package-lock.json or yarn.lock files to identify affected packages, including those nested in dependency trees.

- Search for cached versions of affected dependencies in artifact repositories and dependency management tools.

- Pin npm package dependency versions to known safe releases produced prior to Sept. 16, 2025.

- Immediately rotate all developer credentials.

- Mandate phishing-resistant multifactor authentication (MFA) on all developer accounts, especially for critical platforms like GitHub and npm.

- Monitor for anomalous network behavior.

- Block outbound connections to webhook.site domains.

- Monitor firewall logs for connections to suspicious domains.

- Harden GitHub security by removing unnecessary GitHub Apps and OAuth applications, and auditing repository webhooks and secrets.

- Enable branch protection rules, GitHub Secret Scanning alerts, and Dependabot security updates.

See the following resources for additional guidance on this compromise:

GitHub: Our plan for a more secure npm supply chain

StepSecurity: Shai-Hulud: Self Replicating Work Compromises 500+ NPM Packages
Palo Alto Networks Unit 42: "Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain Attack (Updated September 18)
Socket: Updated and Ongoing Supply Chain Attack Targets CrowdStrike npm Packages
ReversingLabs: Shai-hulud supply chain attack spreads token-stealing malware on npm

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

[i] Ashish Kurmi, "Shai-Hulud: Self Replicating Work Compromises 500+ NPM Packages," StepSecurity, (September 15, 2025), <https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised;> Kush Pandya, Peter van der Zee, and Olivia Brown, "Updated and Ongoing Supply Chain Attack Targets CrowdStrike npm Packages," Socket, (September 16, 2025), <https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages>.

[ii] Palo Alto Networks Unit 42, "'Shai-Hulud' Worm Compromises npm Ecosystem in Supply Chain Attack (Updated September 19)," Unit 42, Palo Alto Networks, (September 17, 2025), <https://unit42.paloaltonetworks.com/npm-supply-chain-attack/>.

[iii] Palo Alto Networks Unit 42, "Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain Attack (Updated September 19)."

<https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem>

Hackers - October 26, 2025, 6:52 am

This is still a problem, I feel like npm/pip/brew/other package managers are one of the best spread methods around right now.