Wird diese Nachricht nicht richtig dargestellt, klicken Sie bitte **hier**.

hvs consulting

# Threat Notification

## Summary

Wiz reports that a new Shai-Hulud campaign surfaced and has already compromised more than 750 npm packages. It is currently still continuing to self-propagate throughout automated build pipelines. [1]
Just like the previous malware, which greatly impacted the npm ecosystem, the new variant harvests credentials (e.g. GitHub tokens, npm tokens, secrets for AWS/Azure/GCP ) which it exfiltrates to attacker controlled infrastructure. Stolen credentials are automatically used to infect packages under the control of the compromised maintainer's account. [1][3]

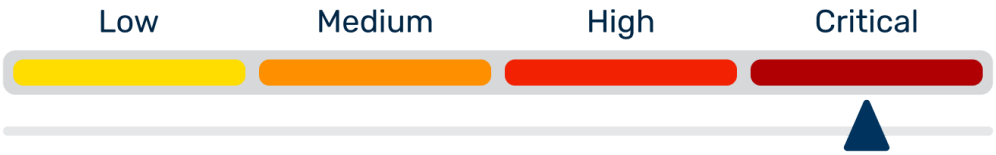
**Indicators of Compromise**

**Threat Hunting Rules**

## Why it matters

- Credential theft & persistent access: Secrets for cloud providers, GitHub repos, and package registries of affected repositories are stolen. The malware's logic has been significantly improved. It now includes a backdoor for built environments that is controlled via GitHub discussions.
- Data Destruction: If the malware fails to find any credentials to steal, it will wipe the current users home folder. [3]
- Supply Chain Cascading Effect: Maintainers’ entire package ecosystems risk compromise via forced npm publishes.
- Persistence: In this current campaign GitHub Actions are abused to GitHub Actions to reinfect repos and continuously exfiltrate credentials.
- Intellectual Property Exposure: The malware changes private repositories to public, risking leakage of sensitive company IPs and proprietary code.

## HvS Risk Assessment




**Definition of HvS Risk Levels:**
Since HvS cannot directly assess the risk specific to your organization, given that it depends on multiple factors such as your security posture, potential exposure, and other considerations, we provide an indicative risk level to guide your reaction time:

- HvS Risk Critical: React immediately
- HvS Risk High: React within 1 week
- HvS Risk Medium: React within 1 month
- HvS Risk Low: React within 6 months

# Our Recommendations

Threat Hunting

- Monitor all repositories for the following malicious files: [1][3]
  - `bun_environment.js`
  - `setup_bun.js`
  - `.github/workflows/discussion.yaml`
  - `.github/workflows/formatter_123456789.yml`
- Monitor all repositories for any branches named `add-linter-workflow-{Date.now()}` [1]
- Scan for the following SHA-1 malware hashes [1]:
  - `d60ec97eea19fffb4809bc35b91033b52490ca11` (`bun_environment.js`)
  - `3d7570d14d34b0ba137d502f042b27b0f37a59fa` (`bun_environment.js`)
  - `d1829b4708126dcc7bea7437c04d1f10eacd4a16` (`setup_bun.js`)
- Review your environment for affected packages. For a recent list refer to [2].

Monitoring

- Monitor your environment for any unexpected Trufflehog executions. While Trufflehog is a legitimate tool for scanning misplaced secrets, the malware abuses it to harvest credentials.[1][4]
- At this time the behaviour of the worm is not yet fully analysed. Therefore it is recommended to actively monitor access to your cloud accounts via public APIs like: [4]
  - secretsmanager.*.amazonaws.com
  - secretmanager.googleapis.com
  - api.github.com/repos

Prevention

- See our September advisory for a full discussion of mid- and long-term measures against software dependency supply chain attacks. [4]

# Sources

[1] Wiz Blog: Shai-Hulud 2.0 - Ongoing Supply Chain Attack

[2] Wiz curated list of compromised npm packages on GitHub

[3] Semgrep Blog: The Second Coming of the npm Worm

[4] HvS Threat-Insights September Advisory

**TLP: AMBER+STRICT**

Publication timestamp: 2025-11-26 09:45 (UTC+1)

---



HvS-Consulting GmbH | Parkring 20 | 85748 Garching | Deutschland / Germany |
+49 89 8906362-0 | welcome@hvs-consulting.de | https://www.hvs-consulting.de

Geschäftsführer / Managing Directors: Frank von Stetten, Markus Pölloth
Handelsregister / Commercial Register: Amtsgericht München, HRB 290304
USt-IdNr. / VAT ID: DE224899823