مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Supply Chain Compromise of npm Package- Bitwarden CLI

Tracking #:432318846

Date:27-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that threat actors attributed to TeamPCP (tracked as @pcpcats) compromised the legitimate Bitwarden CLI npm package, publishing a malicious version @bitwarden/cli@2026.4.0.

TECHNICAL DETAILS:

In April 2026, threat actors attributed to TeamPCP (tracked as @pcpcats) compromised the legitimate Bitwarden CLI npm package, publishing a malicious version @bitwarden/cli@2026.4.0. This package was available on the npm registry for approximately 93 minutes (roughly 5:57 PM to 7:30 PM ET on April 22, 2026) before being detected and removed.
The malware forms part of a broader coordinated supply-chain campaign that also poisoned multiple Checkmarx distribution channels, including Docker Hub images, GitHub Actions, and VS Code extensions. It uses advanced obfuscation, multi-provider credential harvesting (targeting npm tokens, GitHub PATs, cloud secrets, SSH keys, and AI tool configs), worm-like self-propagation, and resilient exfiltration via a primary C2 server and GitHub dead drops.
This incident continues the post-September 2025 Shai-Hulud evolution, shifting npm threats from isolated incidents to systematic, wormable campaigns that weaponize developer and CI/CD trust. Exposure is limited to users who installed the exact malicious version during the narrow window. However, the campaign's wormable nature and targeting of security tooling raise the risk of downstream propagation.

Details
The attack leveraged compromised Checkmarx infrastructure (specifically the checkmarx/ast-github-action used in Bitwarden's CI/CD pipeline) to inject malicious code into the npm publication process. The malicious package impersonates the official Bitwarden CLI while adding execution paths that trigger automatically.

Indicators of Compromise (IoCs):
Network IoCs

- audit.checkmarx[.]cx
- 94.154.172[.]43
- checkmarx[.]cx
- 91.195.240[.]123

GitHub IoCs

- helloworm00/hello-world
- bc544f455d7c06c8a1f3446160a6d9a4a8236b11
- helloworm00@proton[.]me
- LongLiveTheResistanceAgainstMachines:*
- <dune-word>-<dune-word>-<3digits> (repo pattern)
- "Checkmarx Configuration Storage" (repo description)

File Hash IoCs (SHA256)

- f35475829991b303c5efc2ee0f343dd38f8614e8b5e69db683923135f85cf60d (bw_setup.js)
- 18f784b3bc9a0bcdcb1a8d7f51bc5f54323fc40cbd874119354ab609bef6e4cb (bw1.js)
- 167ce57ef59a32a6a0ef4137785828077879092d7f83ddbc1755d6e69116e0ad

(package.json)

File / Artifact IoCs

- bw_setup.js
- bw1.js
- setup.mjs
- .github/workflows/format-check.yml
- format-results (artifact)

npm IoCs

- @bitwarden/cli@2026.4.0
- "preinstall": "node setup.mjs"

RECOMMENDATIONS:

- Check Exposure: Verify if @bitwarden/cli@2026.4.0 was installed (e.g., via npm list @bitwarden/cli or CI logs)
- Rotate Credentials: Immediately rotate all potentially exposed secrets — npm tokens, GitHub PATs, SSH keys, cloud access keys (AWS/Azure/GCP), CI/CD secrets, and AI tool configurations.
- Block known malicious domains/IPs at network perimeter.
- Audit:
  - npm dependencies
  - GitHub repositories
  - CI/CD pipelines

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://unit42.paloaltonetworks.com/monitoring-npm-supply-chain-attacks/