AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Kompromentim i Zinxhirit të Furnizimit nga Paketa npm - Bitwarden CLI

Data: 27/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Aktorët kërcënues të atribuar TeamPCP (të gjurmuar si @pcpcats) kompromentuan paketën legjitime npm Bitwarden CLI, duke publikuar një version keqdashës @bitwarden/cli@2026.4.0.

Informacione Teknike

Në prill të vitit 2026, aktorët kërcënues të atribuar TeamPCP (të gjurmuar si @pcpcats) kompromentuan paketën legjitime npm të Bitwarden CLI, duke publikuar një version keqdashës @bitwarden/cli@2026.4.0.

Kjo paketë ishte e disponueshme në regjistrin e npm për afërsisht 93 minuta (afërsisht nga ora 17:57 deri në 19:30 ET më 22 prill 2026) përpara se të zbulohej dhe hiqej.

Macaueri është pjesë e një fushate më të gjerë të koordinuar të zinxhirit të furnizimit që gjithashtu injektoi shumë kanale shpërndarjeje të Checkmarx, duke përfshirë imazhet Docker Hub, GitHub Actions dhe zgjerimet VS Code. Ai përdor obfuskim të avancuar, mbledhje kredencialesh nga shumë ofrues (duke synuar tokenët npm, PAT-të e GitHub, sekretet e cloud-it, çelësat SSH dhe konfigurimet e mjeteve AI), vetë-përhapje të ngjashme me warn-et dhe ekfiltrim elastik nëpërmjet një serveri primar C2 dhe deaddrop-eve të GitHub.

Ky incident vazhdon evolucionin Shai-Hulud pas shtatorit 2025, duke i zhvendosur kërcënimet npm nga incidente të izoluara në fushata sistematike dhe të warneve që përdorin si armë besimin e zhvilluesve dhe CI/CD.
Ekspozimi është i kufizuar vetëm tek përdoruesit që instaluan versionin e saktë keqdashës gjatë dritares së ngushtë. Megjithatë, natyra e krimbave të fushatës dhe synimi i mjeteve të sigurisë rrisin rrezikun e përhapjes në rrjedhën e poshtme.
Detajet
Sulmi shfrytëzoi infrastrukturën e kompromentuar të Checkmarx (konkretisht veprimin github checkmarx/ast të përdorur në CI/CD të Bitwarden) për të injektuar kod keqdashës në procesin e publikimit npm. Paketa keqdashëse imiton CLI-në zyrtare të Bitwarden ndërsa shton pathe ekzekutimi që aktivizohen automatikisht.

Treguesit e Kompromisit (IoC):
IoC-të e Rrjetit
• audit.checkmarx[.]cx
• 94.154.172[.]43
• checkmarx[.]cx
• 91.195.240[.]123
IoC-të e GitHub
• helloworm00/hello-world

• bc544f455d7c06c8a1f3446160a6d9a4a8236b11
• helloworm00@proton[.]me
• LongLiveTheResistanceAgainstMachines:*
• <fjala-dune>-<fjala-dune>-<3shifra> (model depoje)
• "Ruajtja e Konfigurimit të Checkmarx" (përshkrimi i depoje)
IoC-të e Hash-it të Skedarit (SHA256)
• f35475829991b303c5efc2ee0f343dd38f8614e8b5e69db683923135f85cf60d
(bw_setup.js)
•18f784b3bc9a0bcdcb1a8d7f51bc5f54323fc40cbd874119354ab609bef6e4cb (bw1.js)
•167ce57ef59a32a6a0ef4137785828077879092d7f83ddbc1755d6e69116e0ad

(package.json)

Skedar / Artifakte IoC
• bw_setup.js
• bw1.js
• setup.mjs
• .github/workflows/format-check.yml
• format-results (artifakt)
npm IoCs
• @bitwarden/cli@2026.4.0
• "para-instalim": "nyja setup.mjs

Rekomandime

AKSK rekomandon :

• Kontrolloni Ekspozimin: Verifikoni nëse @bitwarden/cli@2026.4.0 është instaluar (p.sh., nëpërmjet listës npm @bitwarden/cli ose regjistrave CI)
• Rrotulloni Kredencialet: Rrotulloni menjëherë të gjitha informacionet potencialisht të ekspozuara - tokenët npm, PAT-të GitHub, çelësat SSH, çelësat e aksesit në cloud (AWS/Azure/GCP), sekretet CI/CD dhe konfigurimet e mjeteve AI.

• Bllokoni domeinet/IP-të e njohura keqdashëse në perimetrin e rrjetit.
• Auditimi:
o varësitë npm
o depot e GitHub
o CI/CD pipelines