Vulnerability Assessment Report Template

Ime i prezime: Danilo Cvijetic
Tim: 1
Datum: 29.11.2025
Scan Tool: Nessus (10.10.1 (#10) LINUX)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2024-28863

- **Opis:**
  Ranjivost utiče na `node-tar` (paket `tar` za Node.js). Verzije prije **6.2.1** nemaju ograničenje broja pod-foldera (dubine putanje) prilikom raspakivanja. Napadač može kreirati arhivu sa ekstremno velikim brojem ugnježdenih direktorijuma. Prilikom ekstrakcije `node-tar` će alocirati resurse za svaki nivo i može dovesti do velike potrošnje memorije i rušenja Node.js procesa (Denial of Service). Verzija **6.2.1** uvodi validaciju dubine i odbacuje zapise koji prelaze dozvoljenu dubinu.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 6.5 MEDIUM**
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

  AV:N — Attack Vector: Network
  Napad se može izvršiti preko mrežnog interfejsa, bez potrebe za fizičkim pristupom sistemu.

AC:L — Attack Complexity: Low
Eksploatacija ne zahteva specijalne uslove, napadač samo mora dostaviti posebno formiranu `.tar` arhivu.

PR:N — Privileges Required: None
Napadač ne zahteva autentifikaciju niti bilo kakve privilegije da bi započeo napad.

UI:R — User Interaction: Required
Potrebno je da korisnik ili sistem pokrene ekstrakciju arhive kako bi ranjivost bila aktivirana.

S:U — Scope: Unchanged
Napad utiče samo na komponente unutar istog bezbednosnog domena i ne prelazi granicu privilegija drugih sistema.

C:N — Confidentiality Impact: None
Ranjivost ne omogućava pristup poverljivim informacijama.

I:N — Integrity Impact: None
Napadač ne može da izmeni sistemske ili aplikacione podatke.

A:H — Availability Impact: High
Ekstrakcija arhive sa ekstremnom dubinom direktorijuma može dovesti do potpunog iscrpljenja memorije i pada procesa.

- **Opravdanje:**
  Ranjivost omogućava udaljenom napadaču da jednostavnim slanjem zlonamerne `.tar` arhive izazove pad procesa prilikom ekstrakcije, bez potrebe za privilegijama. Eksploatacija zahteva samo da sistem ili korisnik otvore arhivu, što predstavlja jedinu potrebnu interakciju. Uticaj je ograničen na dostupnost servisa, dok poverljivost i integritet ostaju netaknuti.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): NE**
  Iako je ranjivost javno opisana, nema poznatog javnog exploit-skripta koji je dokumentovan
  Bez obzira sto nema javno objavljenog exploit-koda, tehnička priroda problema znači da je relativno jednostavno kreirati zlonamernu arhivu.

Problem je da `node-tar < 6.2.1` ne limitira broj ili dubinu kreiranih pod-direktorijuma prilikom raspakivanja. Napadač može napraviti `.tar` arhivu čiji fajl sadrži veoma duboku putanju — recimo `a/a/a/a/.../a/file.txt`, sa hiljadama (ili više) nivoa. Kad takva arhiva bude raspakovana, `node-tar` će rekurzivno kreirati sve te foldere, što brzo povuče ogromnu potrošnju memorije i CPU. To dovodi do rušenja procesa. (DOS)

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost utiče na `node-tar`. Problem postoji u svim verzijama ≤ 6.2.0 i je ispravljen u verziji 6.2.1 . U kodu koji obrađuje *putanje* i kreira direktorijume pri raspakivanju nije postojala nikakva validacija ili limit za maksimalnu dubinu ugnježdenih direktorijuma. Ovo omogućava napadaču da kroz posebno napravljen `.tar` uzrokuje eksponencijalnu/linearno-veliku alokaciju i iscrpljivanje memorije/CPU (DoS).

  Popravka je dodata uz uvođenje opcije `maxDepth` (podrazumevana vrednost 1024).
  Fix commit je: `fe8cd57da5686f8695415414bda49206a545f7f7`

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): DA**
  Ranjivost je ispravljena od strane maintainer-a biblioteke **node-tar** u verziji **6.2.1**.
  Svi vendor-i i ekosistemi koji koriste `tar` (npm, yarn, pnpm, GitHub Actions runners, CI/CD sistemi, Docker bazirani Node image-ovi) preporučuju ažuriranje na 6.2.1 ili noviju verziju.
- **Mitigation Strategy:**
  Mitigacija se radi azuriranjem problematicnog paketa na verziju >6.2.1. Ukoliko se ovaj paket direktno koristi onda je potrebno direktno instalirati odgovarajucu verziju preko npm, yarn ili pnpm alata. Ukoliko je ovaj paket tranzitivna zavisnost, potrebno je dodati poseban blok u package.json:

  { "overrides": { "tar": "^6.2.1" } }.

  Komande kao sto su npm audit fix takodje mogu automatski detektovati ovu ranjivu verziju i azurirati je. Takodje alati kao sto su GitHub Dependabot mogu automatski napraviti PR i azurirati ovu verziju.

- **Alternativni fix (ukoliko ne postoji vendorski):**

Koriscenje druge biblioteke i onemogucavanje automatskog raspakivanja arhiva u kodu.