Vulnerability Assessment Report Template

Ime i prezime: Miloš Stojanović R2 29/2024
Tim: Tim 10
Datum: 26.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**

  node-tar je paket za Node.js. node-tar pre verzije **6.2.1** nema ograničenja na broj podfoldera kreiranih za vreme kreiranja datoteke. Napadač koji generiše veliki broj podfoldera može da potroši RAM memoriju na sistemu koji pokreće node-tar, pa čak i da sruši Node.js klijent u roku od nekoliko sekundi od pokretanja koristeći putanju sa previše podfoldera.

---

2. CVSS skor

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

  Attack vector: Network – Ranjivost dolazi od paketa sa koji se preuzima sa interneta. Napadač nije primoran da bude fizički blizu sistemu, već ga može napasti preko mreže, a najverovatnije preko interneta.
  Attack complexity: Low – Napadaču nije potrebno mnogo znanja za izvođenje napada. Takođe, sam napad nije previše kompleksan s obzirom na to da je samo potrebno postaviti veliki broj podfoldera pri kreiranju datoteke.
  Privileges Required: None – Napadaču nije potrebna nikakva veza sa sistemom za vršenje napada. Sam napad ne zahteva nikakve privilegije.
  User interaction: Required – Da bi se napad izvršio, potrebno je da korisnik pokrene raspakivanje datoteke.
  Scope: Unchanged – Opseg ranjivosti se ne menja.

Confidentiality: None – Napadom se ne narušava poverljivost podataka pošto ne dolazi do pristupa nedozvoljenim podacima.
Integrity: None – Napadač ne menja podatke niti dolazi u kontakt sa bilo kakvim podacima na sistemu.
Availability: High – Napadač može da zaguši sistem punjenjem RAM memorije i time napravi da sistem postane nedostupan.

- **Opravdanje:**

  Ovim napadom je moguće srušiti node client, a samim tim je moguće i iscrpiti resurse procesora i RAM memorije. U tom slučaju može doći do zamrzavanja sistema kao i prestajanja rada bitnih servisa. Olakšavajuća okolnost je to što je potrebna akcija korisnika da bi se izvršio napad pa postoji mogućnost da će se maliciozni kod primetiti pre pokretanja aplikacije. Nezgodno je to što, ukoliko je maliciozni kod dobro sakriven u aplikaciji ili korisnik nije dovoljno stručan da prepozna maliciozan kod, lako može doći do izvršenja napada. S obzirom na to da nije teško napisati kod koji koristi ovu ranjivost, eksploatabilnost je velika. Ova ranjivost ima potencijal da proizvede situaciju koju napadač može da iskoristi da napravi još veći problem sistemu. Ukoliko se, recimo, korišćenjem ove ranjivosti sruši neki bezbednosni sistem, to ostavlja prostor napadaču da napadne sistem koji je do tada bio zaštićen.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da

  U ovom github issue je dat opis kako se moze iskoristiti ranjivost.

  https://github.com/isaacs/node-tar/security/advisories/GHSA-f5x3-32g6-xq36

- **Opis eksploita:**
  Potrebno je pri kreiranju datoteke specificirati putanju fajla u veliku dubinu. Na primer: root/folder1/folder2/.../folder10000000000/file.txt
  Ovakvim kreiranjem datoteke će se iscrpeti RAM memorija i može doći do zamrzavanja sistema.
- **Kod eksploita (ukoliko postoji):**

  Kod nije preuzet sa github linka. Napisan je prema opisu exploita. Bitno je da se pri kreiranju datoteke prođe kroz for petlju i napravi da putanja do fajla prolazi kroz veliki

broj podfoldera (odnosno u veliku dubinu).

```
function generateDeepNestedFolderStructure() {
  const dirPath = path.join(__dirname, 'deep-nested');
  let nestedDir = dirPath;

  for (let i = 0; i < 1000000000000; i++) {
    nestedDir = path.join(nestedDir, `folder${i}`);
    fs.mkdirSync(nestedDir, { recursive: true });
  }

  tar.c(
    {
      gzip: true,
      file: path.join(__dirname, 'deep-nested.tar.gz'),
      cwd: dirPath,
    },
    ['.']
  ).then(() => {
    console.log('Tar file created successfully!');
  });
}
```

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Ranjivost postoji od prve verzije node-tar paketa sve do verzije 6.2.1 kada je uveden fix. Problem je to što nije postojala provera za dubinu podfoldera pri kreiranju datoteke pa je time praktično bilo dozvoljeno kreiranje datoteke sa beskonačnom dubinom. Problem je rešen tako što je uvedena granica za dubinu. Podrazumevano je podešena na 1024, ali se može menjati i ukinuti (postavljanjem vrednosti na “Infinity”).

- **Primer Koda (ako je primenljivo):**

```
                                                  51 + const DEFAULT_MAX_DEPTH = 1024
51
52      // Unlinks on Windows are not atomic.     53      // Unlinks on Windows are not atomic.
53      //                                        54      //
        @@ -181,6 +182,12 @@ class Unpack extends Parser {
181         this.processGid = (this.preserveOwner ||  182         this.processGid = (this.preserveOwner ||
        this.setOwner) && process.getgid ?                this.setOwner) && process.getgid ?
182           process.getgid() : null                 183           process.getgid() : null
183                                                   184
                                                    185 +     // prevent excessively deep nesting of subfolders
                                                    186 +     // set to `Infinity` to remove this restriction
                                                    187 +     this.maxDepth = typeof opt.maxDepth === 'number'
                                                    188 +       ? opt.maxDepth
                                                    189 +       : DEFAULT_MAX_DEPTH
                                                    190 +
```

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**

  Potrebno je odraditi instalaciju ili update paketa na verziju iznad 6.2.0. To se može uraditi komandom: **npm install tar@6.2.1**

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

  Problem bi se rešio tako što se izmeni paket i uvede granica za dubinu i provera te granice prilikom kreiranja datoteke.