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-2017-16548
- **Opis:**
  Ranjivost pogadja rsync verzije < 3.12 i <3.13-dev. Tip ranjivosti je heap-based buffer over-read.
  Ranjivost u funkciji `receive_xattr()` omogućava napadaču da pošalje maliciozan rsync paket koji sadrži “extended attribute name” bez null-terminatora (\0). Pošto rsync ne proverava dužinu i validnost ovakvog imena, funkcija čita izvan granica heap buffera. Time dolazi do DoS pada rsync procesa, a u određenim konfiguracijama potencijalno i do nepredviđenih efekata.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 9.8 (Critical)
- **Vektor: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

- **AV:N — Network:** Napad se izvodi preko mreže koristeći rsync protokol.
- **AC:L — Low complexity:** Potreban je samo crafted paket bez dodatnih uslova.
- **PR:N — No privileges:** Nije potrebna autentifikacija za slanje paketa.
- **UI:N — No user interaction:** Korisnik ne mora učiniti ništa; rsync obradi paket automatski.
- **S:U — Unchanged:** Napad utiče na isti sigurnosni domen (proces rsync-a).
- **C:H — High confidentiality impact:** Ako dođe do memory exposure (over-read), moguće curenje podataka.
- **I:H — High integrity impact:** Memory corruption može promeniti stanje procesa.
- **A:H — High availability impact:** rsync proces može pasti, gubitak dostupnosti.

- **Opravdanje:**
  Napad je trivijalno izvodljiv preko mreže i ne zahteva privilegije ni interakciju korisnika. Greška dovodi do čitanja izvan heap buffera, što uzrokuje pad rsync-a i može ugroziti poverljivost ili integritet. Zbog visokog uticaja na sve tri komponente (CIA), CVSS skor 9.8 je opravdan.

---

3. Dostupnost eksploita

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

  U javnim resursima nije objavljen direktan PoC exploit kod za potpuno iskorišćavanje ranjivosti.
  Međutim, tehnička priroda greške čini DoS PoC trivijalnim za kreiranje. Dovoljno je poslati rsync paket sa xattr name poljem bez null-terminatora.

  Zbog toga se u praksi smatra da eksploitabilnost postoji, iako se javno ne dijeli PoC.

  Napadač šalje rsync paketu manipulisan “extended attribute name” (`xattr name`) polje u kojem nedostaje završni NULL (`\0`). Funkcija `receive_xattr()` kopira ovo ime u lokalni heap buffer, ali se oslanja na deklarisanu dužinu koja može biti veća od buffera i ne proverava terminator. Rezultat je heap over-read → pad rsync procesa.

---

4. Analiza uzroka (root cause)

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

- Greška potiče iz funkcije: **`receive_xattr()`** u fajlu **`xattrs.c`**.
- U verzijama **3.1.2** i **3.1.3-dev**, rsync nije proveravao:
  - da li je `name_len` unutar granica buffera,
  - da li je xattr ime pravilno završeno null-terminatorom.

  Ovaj propust dovodi do čitanja izvan heap buffera kada se kopira xattr ime. Zvanični patch je kasnije integrisan u rsync paket preko distribucija, i poznato je da je ranjivost popravljena u sigurnosnim ažuriranjima za Debian/Ubuntu/RedHat kroz 2018. Godinu.

  Commit koji je popravio gresku je: `47a63d90e71d3e19e0e96052bb8c6b9cb140ecc1`

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): DA**
  Distribucije (Debian, Ubuntu, RedHat, SUSE…) su objavile zakrpe kroz njihove repozitorijume paketa.
  rsync 3.2.x i vise verzije nisu ranjivi.

- **Mitigation Strategy:**
  Mitigacija se obavlja azuriranjem ranjivog paketa na verziju > 3.1.2. To se moze odraditi preko package managera za konkretan operativni sistem ili automatizovati azuriranje preko mreze za grupu racunara.

- **Alternativni fix (ukoliko ne postoji vendorski):**
  Iskljuciti extented attributes za rsync:
  rsync –no-xattrs

  dozvoliti pristup samo sa whitelist ip adresa

  iskljuciti rsync daemon potpuno:
  systemctl disable rsync.service