Vulnerability Assessment Report Template

Ime i prezime: Dušica Trbović
Tim: ?
Datum: 21.12.2025.
Scan Tool: Nessus (10.11.1 (#21) LINUX)
Test okruženje: Metasploitable3

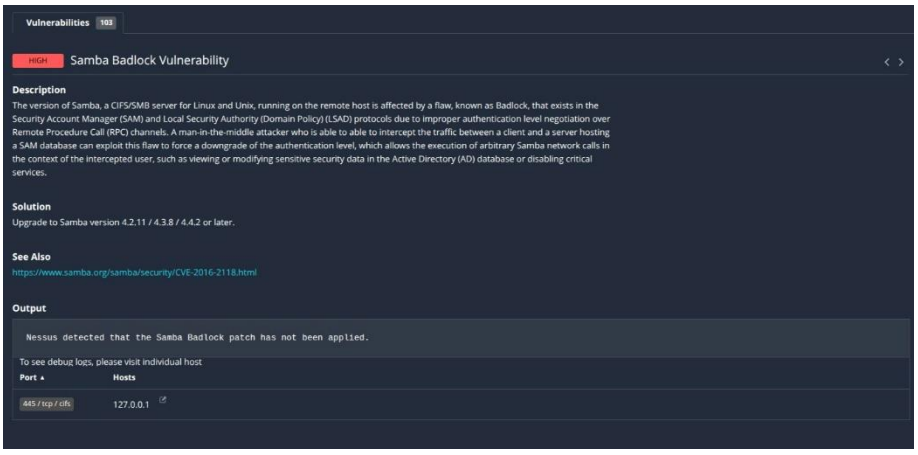
---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2016-2118
- **Opis:**
  Ranjivost Samba Badlock (CVE-2016-2118) pogađa Samba servis, koji implementira SMB/CIFS protokol za deljenje fajlova i mrežnu autentifikaciju na Linux i Unix sistemima. Ranjivost se odnosi na način na koji Samba obrađuje autentifikaciju preko RPC (Remote Procedure Call) kanala, konkretno u komunikaciji sa Security Account Manager (SAM) i Local Security Authority (LSAD) servisima.

  Napadač koji je u poziciji man-in-the-middle (MITM) može iskoristiti ovu ranjivost da izvrši downgrade autentifikacionog nivoa, čime se omogućava izvršavanje proizvoljnih Samba mrežnih poziva u kontekstu legitimnog korisnika. Kao posledica, napadač može pristupiti ili izmeniti osetljive podatke, uključujući korisničke naloge, sigurnosne politike i Active Directory informacije, kao i onemogućiti ključne servise.

  Ranjivost se manifestuje na SMB portu 445/tcp, a pogođeni servis je Samba server koji koristi ranjive verzije softvera bez primenjenog bezbednosnog zakrpa (patch-a).



---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 7.5 (High)
- **Vektor**: AV:N / AC:H / PR:N / UI:N / S:U / C:H / I:H / A:H
- **Objašnjenje komponenti:**
  - **AV:N (Network)**
    - Napad se može izvesti udaljeno preko mreže, bez fizičkog pristupa sistemu.
  - **AC:H (High)**
    - Za uspešan napad potrebni su specifični uslovi, poput pozicije napadača u MITM scenariju, što povećava kompleksnost napada.
  - **PR:N (None)**
    - Napadaču nisu potrebne privilegije na ciljnom sistemu pre izvođenja napada.
  - **UI:N (None)**
    - Nije potrebna interakcija korisnika.
  - **S:U (Unchanged)**
    - Uticaj ranjivosti je ograničen na isti bezbednosni domen.
  - **C:H (High)**
    - Moguć je potpuni kompromis poverljivosti podataka.
  - **I:H (High)**
    - Moguć je neovlašćen pristup i izmena podataka.
  - **A:H (High)**
    - Postoji mogućnost ozbiljnog narušavanja dostupnosti servisa.

- **Opravdanje:**
  Zašto Ranjivost CVE-2016-2118 (Samba Badlock) dobija visok CVSS skor zbog činjenice da omogućava ozbiljan kompromis poverljivosti, integriteta i dostupnosti sistema. Napad se može izvesti udaljeno, bez autentifikacije i bez interakcije korisnika, što značajno povećava potencijalni uticaj.

  Ipak, visoka kompleksnost napada (AC:H) umanjuje bazni CVSS skor, jer napadač mora biti u poziciji da presreće mrećni saobraćaj između klijenta i servera (MITM scenario). Uprkos tome, uspešna eksploatacija može dovesti do izvršavanja proizvoljnih mrežnih operacija u kontekstu legitimnog korisnika, pristupa osetljivim podacima i destabilizacije sistema.

3. Dostupnost eksploita

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

  Za ranjivost CVE-2016-2118 (Samba Badlock) postoje javno dostupni tehnički opisi napada, proof-of-concept alati i detaljna dokumentacija, ali ne postoji trivijalan „one-click“ exploit koji omogućava direktno izvršavanje koda bez dodatnih uslova.

- **Opis eksploita:**
  Eksploatacija ove ranjivosti zasniva se na downgrade napadu autentifikacije u Samba SMB/CIFS implementaciji. Napadač, koji se nalazi u poziciji man-in-the-middle (MITM) između klijenta i Samba servera, može manipulisati RPC komunikacijom i primorati sistem da koristi slabiji nivo autentifikacije.
  Uspešnim napadom moguće je:
  - izvršavanje proizvoljnih Samba mrežnih operacija,
  - neovlašćen pristup osetljivim podacima,
  - izmena sigurnosnih podešavanja,
  - potencijalno narušavanje Active Directory okruženja ili gašenje kritičnih servisa.

  Napad ne zahteva validne korisničke kredencijale, ali zahteva specifične mrežne uslove i aktivno presretanje saobraćaja, što značajno utiče na kompleksnost eksploatacije.

- **Kod eksploita (ukoliko postoji):**
  Ne postoji jednostavan javni exploit u vidu Metasploit RCE modula. Međutim, dostupni su:
  - proof-of-concept skripti,
  - istraživački alati za simulaciju downgrade napada,
  - detaljni tehnički opisi napada u okviru bezbednosnih izveštaja i akademskih analiza.

  Eksploatacija se u praksi najčešće izvodi kombinacijom mrežnih alata za presretanje saobraćaja (npr. ARP spoofing) i prilagođenih skripti koje manipulišu RPC komunikacijom.

---

4. Analiza uzroka (root cause)

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

Ranjivost Samba Badlock (CVE-2016-2118) nije posledica klasične programske greške poput buffer overflow-a ili pogrešne validacije ulaza, već predstavlja dizajnerski propust u načinu na koji Samba implementira autentifikaciju i autorizaciju u okviru RPC komunikacije.

Problem je prisutan u verzijama Samba servera pre 4.4.2, 4.3.8 i 4.2.11, gde je dozvoljeno neadekvatno pregovaranje nivoa autentifikacije između klijenta i servera. Tokom inicijalne faze RPC komunikacije, napadač u poziciji man-in-the-middle može namerno izazvati downgrade autentifikacionog mehanizma, čime se zaobilaze bezbednosne provere koje bi inače bile primenjene.

Kao posledica toga, Samba server prihvata RPC zahteve sa nižim nivoom zaštite, što omogućava neovlašćeno izvršavanje određenih operacija nad SAM/LSAD servisima. Ovaj propust je rezultat nedovoljno striktne kontrole bezbednosnih zahteva u protokolu, a ne pojedinačnog pogrešnog commita.

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

Za ovu ranjivost ne postoji konkretan, izolovan deo izvornog koda koji se može izdvojiti kao jedini uzrok problema. Ranjivost proizilazi iz kombinacije protokolskih odluka i implementacije RPC autentifikacije, zbog čega se ne manifestuje kroz jednostavan kodni primer.

Eksploatacija se zasniva na manipulaciji mrežnog saobraćaja i pregovaranja parametara autentifikacije, a ne na direktnom iskorišćavanju funkcije ili metode u kodu. Zbog toga se u javno dostupnim analizama fokus stavlja na tok komunikacije i dizajn protokola, a ne na konkretan programski segment.

---

5. Preporuke za mitigaciju

- **Da li je dostupan vendor fix ili patch (Da/Ne):**

  Da.
  Zvanični vendor patch je dostupan i objavljen od strane Samba tima. Problem je rešen u verzijama Samba 4.4.2, 4.3.8 i 4.2.11, koje uvode strožu kontrolu autentifikacije i sprečavaju nebezbedno pregovaranje nivoa bezbednosti tokom RPC komunikacije.

- **Mitigation strategy:**

  Preporučena i najefikasnija mera mitigacije jeste nadogradnja Samba servera na verziju koja sadrži zvanični bezbednosni patch. Time se onemogućava downgrade autentifikacije i sprečava neovlašćeni pristup RPC servisima.

  Konkretni koraci uključuju:

  - Proveru trenutne verzije Samba servera (smbd --version)
  - Ažuriranje paketa putem zvaničnog package manager-a operativnog sistema
  - Restartovanje Samba servisa nakon primene patch-a

  U produkcionim okruženjima, preporučuje se korišćenje automatizovanih alata za upravljanje zakrpama (npr. Ansible, Puppet, Chef), kako bi se obezbedila dosledna i pravovremena primena bezbednosnih ispravki.

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

  U slučajevima kada nadogradnja nije odmah moguća, mogu se primeniti privremene kompenzacione mere, iako one ne predstavljaju trajno rešenje. Te mere uključuju:

  - Onemogućavanje ili ograničavanje RPC servisa koji nisu neophodni
  - Restrikciju pristupa SMB/RPC portovima (npr. 445/tcp) pomoću firewall pravila
  - Segmentaciju mreže kako bi se sprečio man-in-the-middle napad

- Ograničavanje Samba servisa samo na pouzdane klijente

Ipak, ove mere samo umanjuju rizik i ne uklanjaju osnovni uzrok ranjivosti, zbog čega se smatraju privremenim rešenjem dok se ne primeni zvanični patch.