Vulnerability Assessment Report Template

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

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2008-5161**

- **Opis:**
  Ranjivost pogađa SSH servere koji koriste Cipher Block Chaining (CBC) način enkripcije, uključujući OpenSSH 4.7p1 i druge verzije SSH Tectia servera. Ova ranjivost omogućava remote neautentifikovanom napadaču da pronađe određene tekstualne podatke iz šifrovanog teksta u SSH sesiji koristeći napad na osnovu greške. SSH server standardno sluša na TCP portu 22. Ranjivost predstavlja curenje informacija gde napadač može da rekonstruiše delove otvorenog teksta iz šifrovanog saobraćaja bez direktnog pristupa ključevima enkripcije. Link

  CBC je način enkripcije gde svaki blok šifrovanog teksta zavisi od prethodnog. Ranjivost postoji zbog neadekvatne obrade grešaka u SSH protokolu koja omogućava napadaču da kroz specifične napade otkrije delove otvorenog teksta. Napadač šalje posebno konstruisane pakete i analizira kako server odgovara na greške. Time može da ekstraktuje bitove otvorenog teksta blok po blok.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 3.7 (Low)**
- **Vektor:**
  CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

  AV:N (Attack Vector: Network) - Napad je moguć sa mreže, SSH sluša na portu 22
  AC:H (Attack Complexity: High) - Napad zahteva veoma specifične uslove i preciznu vremensku koordinaciju
  PR:N (Privileges Required: None) - Napadač ne mora biti autentifikovan, ranjivost je

dostupna anonimnom napadaču
UI:N (User interaction: None) - Nije potrebna interakcija korisnika, napad se izvršava
S:U (Scope: Unchanged) - Uticaj je ograničen na SSH sesiju
C:L (Confidentiality: Low) - Napadač može da otkrije samo delove otvorenog teksta, ne kompletan sadržaj sesije, ograničeno curenje podataka
I:N (Integrity: Low) - Nema mogućnosti promene podataka
A:N (Availability: None) - Nema uticaja na dostupnost SSH servisa

- **Opravdanje:**
  Skor 3.7 odražava činjenicu da je napad izuzetno kompleksan za izvršenje. Mada je napad bez autentifikacije i sa mrežnog pristupa, uticaj je minimalan jer napadač može otkriti samo delove podataka. Ova ranjivost je poznata kao teoretski napad i retko je korišćena u praksi zbog svoje kompleksnosti.

---

3. Dostupnost eksploita

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

- **Opis eksploita:**
  Eksploiti za ovu ranjivost zahtevaju detaljno razumevanje CBC kriptografije i SSH protokola. Napad se izvršava tako što napadač šalje specijalno konstruisane SSH pakete i prati kako server obrađuje greške, omogućavajući mu da kroz "plaintext recovery" tehnike rekostruiše delove otvorenog teksta. Neki javni PoC-ovi demonstriraju napade na starije verzije OpenSSH (4.7p1).

  Eksploatacija u praktičnim uslovima se najčešće svodi na detekciju ranjive verzije OpenSSH (npr. 4.7p1) i kombinovanje te informacije sa drugim tehnikama (brute force/credential stuffing) kako bi se dobio pristup sistemu. Priloženi PoC skript automatski proverava da li je meta OpenSSH_4.7p1 i, ako jeste, pokreće Metasploit modul auxiliary/scanner/ssh/ssh_login za pokušaj autentifikacije nad ranjivim serverom.
- **Kod eksploita (ukoliko postoji):**
  GitHub OpenSSH 4.7p1 Exploit

---

4. Analiza uzroka (root cause)

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

  Ranjivost je prisutna u OpenSSH verzijama 4.7p1 i ranijim, kao i u SSH Tectia Server verzijama 4.0 kroz 5.3.8. Problem je u neadekvatnoj obradi grešaka u SSH protokolu kada se koristi CBC način enkripcije.

Greška leži u tome što SSH server ne štiti dovoljno od napada koji manipuliraju CBC blokovima. CBC način rada enkripcije koristi povratnu vezu između blokova gde svaki blok šifrovanog teksta zavisi od prethodnog. Međutim, kada server greško obradi ili neadekvatno validira SSL/TLS handshake ili MAC (Message Authentication Code) greške, omogućava napadaču da kroz specifičnim zahtevima otkrije informacije o otvorenom tekstu.

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

  Tačan kod greške nije javno objavljen, ali problem je u SSH protokol rukovanja sa greškom enkripcije. Rešenje je došlo kroz ažuriranje na verzije koje koriste CTR mod umesto CBC ili sa poboljšanom validacijom greške. Link

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
  - Ažuriranje softvera: Ažurirati na OpenSSH 5.2 ili noviju verziju gde je ova ranjivost ispravljena.
  - Zamena enkripcije: Koristiti CTR mod enkripcije umesto CBC moda. CTR je otporniji na ovaj tip napada.

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

  Pošto je vendor patch dostupan, primarna preporuka je nadogradnja. Ukoliko nadogradnja nije trenutno moguća:

  - Onemogućiti sve CBC šifre u konfiguraciji SSH servera
  - Ograničiti SSH pristup samo sa pouzdanih IP adresa koristeći firewall