Vulnerability Assessment Report Template

Ime i prezime: Ana Tamindžija
Tim:
Datum: 7.12.2025.
Scan Tool: Nessus (10.11.1)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- Opis ranjivosti:

Ova ranjivost se odnosi na **SSH protokol**, konkretno kada se koristi **CBC (Cipher Block Chaining)** mod za šifrovanje podataka u toku SSH sesije.

CBC mod je šifarski način rada koji povezuje šifrovanje svakog bloka sa prethodnim blokom, čime povećava sigurnost. Međutim, ako nije pravilno implementiran (npr. bez odgovarajuće zaštite od grešaka u paddingu), omogućava tzv. **padding oracle napade**, u kojima napadač može analizirati odgovore servera na loše šifrovane poruke i tako postepeno rekonstruisati **dijelove originalnog (plaintext) podatka**.

- **Servis koji je pogođen:**

Na Metasploitable3 sistemu, SSH servis (port **22/tcp**) podržava CBC algoritme poput:

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc

što je direktno povezano sa ovom ranjivošću.

To znači da je server konfigurisan da koristi zastarjele i nesigurne algoritme CBC moda, što direktno omogućava potencijalno iskorišćavanje **CVE-2008-5161**.

Dodatne informacije o pogođenim softverima:

Prema bazi podataka CVE detalja i NVD:

- Pogođene su stare verzije OpenSSH (npr. **OpenSSH 4.7p1**) i **SSH Tectia Client 4.0–4.3.10-K**
- Ranjivost je objavljena još 2008, ali se može detektovati i na modernim sistemima ako konfiguracija koristi nasleđene šifre

Ranjivost CVE-2008-5161 omogućava napadaču da pomoću pasivnog snimanja i manipulacije šifrovanim porukama dođe do dijela osjetljivih podataka unutar SSH sesije, ako server koristi **CBC algoritme**. Ova ranjivost postoji i na analiziranom sistemu jer je prikazano da koristi upravo te algoritme.

---

2. CVSS skor

- **CVSS skor (v3.0): 3.7 (Low)**
- **Vektor:**
  CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Komponenta	Oznaka	Značenje
AV (Attack Vector)	**N** (Network)	Ranjivost se može iskoristiti **daljinski preko mreže**, bez fizičkog pristupa sistemu.
AC (Attack Complexity)	**H** (High)	Za eksploataciju su potrebni **složeni uslovi**, poput naprednog znanja o kriptografiji i sposobnosti analize odgovora servera.
PR (Privileges Required)	**N** (None)	Napadač **ne mora imati nikakve privilegije** na sistemu da bi pokušao napad.
UI (User Interaction)	**N** (None)	**Nema potrebe za interakcijom korisnika** – napad je u potpunosti pasivan/automatski.
S (Scope)	**U** (Unchanged)	Napad ostaje u okviru istog bezbednosnog domena – nema

Komponenta	Oznaka	Značenje
		efekta van zahvaćenog komponenta.
C (Confidentiality Impact)	**L** (Low)	Može doći do **ograničenog curenja podataka** (npr. delimična dešifrovanja paketa).
I (Integrity Impact)	**N** (None)	Ne utiče na integritet – podaci se ne mogu izmeniti.
A (Availability Impact)	**N** (None)	Ne utiče na dostupnost – server ne pada niti postaje nedostupan.

- **Opravdanje:**

  CVSS skor je **relativno nizak (3.7)** jer je **eksploatacija moguća, ali teška** – zahteva napredne tehnike kao što su **padding oracle** napadi i pristup enkriptovanom prometu. **Uticaj je ograničen samo na delimično curenje podataka** (nema uticaja na integritet ili dostupnost). **Nema potrebe za privilegijama niti korisničkom interakcijom**, što podiže ozbiljnost, ali se to ublažava kompleksnošću napada.

  U suštini, iako tehnički ozbiljna, ranjivost se **rijetko uspješno eksploatiše u stvarnim uslovima**, pa se klasifikuje kao niskorizična ali zahteva mitigaciju jer otvara prostor za sofisticiranog napadača.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da. Na GitHub-u postoji više alata koji identifikuju i pomažu u testiranju CVE-2008-5161, uključujući: openSSH.py skripta koja koristi Metasploit-ov ssh_login modul za credential auditing ciljeva sa verzijom OpenSSH 4.7p1. Ovo je poznato kao "audit helper", a ne kao direktna implementacija CBC napada.
- **Opis eksploita:**
  Ova skripta koristi Python biblioteku **pwntools** da:
  - Ostvari vezu sa SSH serverom i provjeri banner verziju (OpenSSH_4.7p1).
  - Ako je ranjiva verzija potvrđena, automatski pokreće **Metasploit** i koristi auxiliary/scanner/ssh/ssh_login modul.

    - Iz datoteke sa kombinacijama korisničkih imena i lozinki (userpass_file) pokušava prijavljivanje dok ne dođe do uspjeha.
    - Prikazuje sesiju i interaktivno je otvara ako login uspije.

  Napad cilja slabosti starog SSH servera (verzija 4.7p1), koji koristi CBC mod, ali glavna svrha je automatizovani credential bruteforce audit, a ne CBC exploit sam po sebi - originalni CBC napad je kriptoanalitički i kompleksan za implementaciju van teorijskog okruženja.

- **Kod eksploita (ukoliko postoji):**

  Repozitorijum: [talha3117/OpenSSH-4.7p1-CVE-2008-5161-Exploit: CVE-2008-5161 OpenSSH 4.7p1 Audit Helper Automates version checking and credential auditing of legacy OpenSSH 4.7p1 (Debian-8ubuntu1) targets by driving Metasploit's auxiliary/scanner/ssh/ssh_login module from Python via pwntools.]

---

4. Analiza uzroka (root cause)

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

  Opis CVE-2008-5161 potvrđuje da ranjivost potiče iz samog načina na koji CBC mod šifrovanja funkcioniše u okviru SSH protokola. Ranjivost je prisutna u više implementacija (npr. OpenSSH, SSH Tectia Client and Server) i u raznim verzijama, uključujući OpenSSH 4.7p1 i druge. Nema specifičnog commit-a, već je slabost ugrađena u dizajn protokola. S obzirom da se ranjivost oslanja na mogućnost oporavka delimičnog plaintext sadržaja iz šifrovanog bloka (ciphertext), uz manipulaciju greškama u CBC režimu, klasifikuje se kao kriptografska dizajnerska slabost, a ne kao implementacijski bug.

  Greška proizilazi iz **nedoslednog ponašanja servera** prilikom obrade loše šifrovanih paketa – server razlikuje greške u **padding-u** i greške u **MAC-u (Message Authentication Code)**, što omogućava tzv. **padding oracle** napade.

  Problem nije vezan za tačno jedan commit, već za **način na koji CBC mod dešifruje podatke** bez prethodne MAC validacije, čime omogućava curenje podataka iz šifrovanih paketa (djelimični plaintext recovery).

---

5. Preporuke za mitigaciju

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

  Da. OpenSSH tim i brojni vendori (npr. Red Hat putem RHSA-2009:1287) su objavili bezbjednosne ispravke koje umanjuju ili u potpunosti uklanjaju ranjivost. Konkretno, u verziji OpenSSH 5.2 i kasnijim implementirano je preferiranje sigurnijih modova šifrovanja (CTR) u odnosu na ranjive CBC modove.

- **Mitigation Strategy:**

  Primarna preporuka je nadogradnja na OpenSSH verziju 5.2 ili noviju, čime se problem direktno eliminiše. Neke od dodatnih konfiguracijskih mjera(ako patch nije moguć) je:

  - Onemogućavanje CBC modova u konfigurafionom fajlu SSH servera (/etc/ssh/sshd_config) kroz postavljanje:
    Ciphers aes128-ctr,aes192-ctr,aes256-ctr
  - Restart sshd servisa nakon izmjena:
    sudo systemctl restart sshd

  Organizacione mjere: Skeneri ranjivosti treba redovno da provjeravaju prisustvo OpenSSH verzija starijih od 5.2. Korisničke sesije treba šifrovati dodatnim slojem zaštite (npr. VPN tunel). Segmentacija mreže kako bi se spriječio man-in-the-middle položaj napadača.

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

  Ukoliko ne postoji mogućnost za patch, mogu se primeniti sledeće alternativne mjere:

- **Ručno onemogućiti CBC šifre** u konfiguraciji (kao iznad).
- **Ograničiti mrežni pristup SSH servisu** samo na poznate i bezbjedne adrese/IP opsege (npr. korišćenjem firewall-a ili VPN-a).
- **Praćenje i analiza saobraćaja** putem IDS/IPS sistema (npr. Snort, Suricata) za detekciju pokušaja napada na SSH sesije.
- **Praćenje logova** za neobične pokušaje konekcije ili greške vezane za padding.