Vulnerability Assessment Report Template

Ime i prezime: Andjela Vukosav

Tim:

Datum: 09.12.2025.

Scan Tool: Nessus (verzija)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

• **CVE ID: CVE-2023-48795 (SSH Terrapin Prefix Truncation Weakness)**

• **Opis:** Ova ranjivost, poznata kao **Terrapin** napad, pogađa **SSH protokol** koji koristi OpenSSH server (i druge implementacije) kada je omogućena podrška za određene algoritme kao što su ChaCha20-Poly1305 i Encrypt-then-MAC (ETM) verzije HMAC algoritama. Ranjivost omogućava man-in-the-middle (MitM) napadaču da manipulacijom paketa u fazi inicijalnog SSH rukovanja zaobiđe određene integritetne kontrole, što može dovesti do snižavanja nivoa sigurnosti konekcije (security downgrade). Konkretno, napadač može izvršiti prefix truncation napad, u kojem preskače dijelove pregovora o ekstenzijama između klijenta i servera, što rezultuje različitim interpretacijama sigurnosnih funkcija sa obje strane konekcije. Time se omogućava uspostavljanje SSH sesije sa oslabljenim sigurnosnim mehanizmima, bez znanja korisnika. U kontekstu testiranog okruženja, ranjivost je otkrivena na OpenSSH servisu verzije < 9.6, koji je aktivan na portu 22 (TCP) hosta sa IP adresom 192.168.56.101. Navedeni server podržava problematične algoritme: ChaCha20-Poly1305, HMAC-SHA256, HMAC-SHA512, HMAC-SHA1. Time se potvrđuje da je server ranjiv na Terrapin napad, jer koristi upravo one kriptografske algoritme koji ne pružaju zaštitu protiv manipulacije u fazi rukovanja (negotiation) i ne implementira striktne mjere za razmjenu ključeva.

2. CVSS skor

• **CVSS skor (numerička vrednost): 5.9 (Medium) – CVSS v3.0**

• **Vektor**: ***CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N***

- **AV:N (Attack Vector – Network):** Napad se može izvesti isključivo putem mreže, jer Terrapin cilja na SSH konekcije (port 22/TCP) i ne zahtijeva fizički pristup mašini.
- **AC:H (Attack Complexity – High):** Eksploatacija zahtijeva specifične uslove – napadač mora biti pozicioniran između klijenta i servera (MitM), te precizno manipulisati sa početnim SSH paketom bez izazivanja greške, što znatno povećava složenost napada.
- **PR:N (Privileges Required – None):** Napadaču nisu potrebne autentifikacione privilegije niti pristup sistemu – dovoljan je pristup mrežnom saobraćaju.
- **UI:N (User Interaction – None):** Nije potrebna nikakva interakcija korisnika – kompromitacija se dešava tokom početne faze SSH pregovora.
- **S:U (Scope – Unchanged):** Ranjivost se ograničava na SSH sesiju i ne prelazi na druge sisteme ili komponente.
- **C:N (Confidentiality – None):** Ranjivost ne omogućava direktan pristup osjetljivim podacima – sadržaj komunikacije ostaje šifrovan i napadač ga ne može dešifrovati bez dodatnih napada.
- **I:H (Integrity – High):** Manipulacijom pregovaračke faze SSH protokola, napadač može oslabiti sigurnosne mehanizme (npr. zaobići određene MAC provjere), čime se ozbiljno narušava integritet sesije i otvara prostor za dalju eksploataciju.
- **A:N (Availability – None):** Napad ne utiče na dostupnost sistema – ne izaziva pad servisa.

• **Opravdanje:** Terrapin ranjivost omogućava man-in-the-middle napadaču da manipuliše inicijalnu SSH razmjenu poruka (handshake) kako bi degradirao sigurnosne funkcije veze, bez da klijent ili server primijete napad. Iako ne omogućava direktnu krađu podataka ni pristup sistemu, predstavlja ozbiljnu prijetnju po integritet SSH sesije, jer otvara mogućnost za dalji napredni napad. Zbog toga je impact na integritet ocijenjen kao visok (I:H), dok je konfidencijalnost i dostupnost nepromijenjena, a kompleksnost napada visoka, što rezultuje CVSS ocjenom 5.9 (Medium).

3. Dostupnost eksploita

• **Postoji javno dostupan eksploit (Da/Ne):** Da.

• **Opis eksploita:** Postoji više javno dostupnih Proof-of-Concept (PoC) eksploita za Terrapin napad, objavljenih na GitHub-u i drugim bezbjednosnim forumima. Eksploatacija funkcioniše tako što napadač mora biti pozicioniran između SSH klijenta i servera (MitM) i koristi tzv. prefix truncation tehniku kojom modifikuje početne pakete tokom SSH „handshake“ faze. Eksploit skraćuje (truncira) poruke pregovora o ekstenzijama, čime omogućava da klijent i server ne razmijene ispravne informacije o podržanim algoritmima (kao što su MAC, KEX ili autentifikacione opcije). Ako server

koristi algoritme kao što su ChaCha20-Poly1305 ili ETM verzije, napadač može zaobići integritet komunikacije, degradirati sigurnosni kontekst i otvoriti prostor za dalju manipulaciju.

• **Kod eksploita (ukoliko postoji):** Sljedeći isječak prikazuje osnovnu logiku eksploita: napadač koristi proxy i posebno pripremljeni modul koji modifikuje dužinu SSH poruka (`SSH_MSG_EXT_INFO`) i eliminiše dio sadržaja kako bi server i klijent imali različito razumijevanje o sigurnosnim mehanizmima:

```
prefix_length = calculate_prefix_truncation_offset()

intercepted_packet = intercept_initial_packet()

truncated_packet = intercepted_packet[prefix_length:]

forward_to_server(truncated_packet)
```

U praksi, ovaj kod funkcioniše kao **"middlebox"** između klijenta i servera, gdje se specijalno izračunava i uklanja određeni broj bajtova iz paketa (`prefix truncation`), a potom se izmijenjeni paket šalje serveru.

4. Analiza uzroka (root cause)

• **Uvođenje Greške (Commit/Verzija):** Greška potiče iz načina na koji su implementirane **SSH Binary Packet Protocol** (BPP) ekstenzije u OpenSSH-u, konkretno u algoritmima ChaCha20-Poly1305 i CBC *Encrypt-then-MAC* varijantama. Istraživači koji su otkrili Terrapin navode da je ranjivost rezultat nedovoljno stroge validacije sekvencijalnih brojeva i nepravilnog tretiranja „padding-a" i prefiksa tokom pregovora (`handshake`) u SSH protokolu. Ova funkcionalnost uvedena je u OpenSSH ekstenzijama koje su postojale godinama (OpenSSH 6.x – 9.5), ali zbog načina implementacije nije bila primijećena sve do kraja 2023. godine. Problem je ispravljen tek u verziji OpenSSH 9.6 (security patch 18.12.2023.), koja uvodi *strict key exchange countermeasures*, dodatne provjere i detekciju prefix truncation pokušaja. Drugim riječima: problem nije samo u jednoj liniji koda, već u dizajnu načina na koji OpenSSH implementira kriptografske ekstenzije i kako povezuje MAC validaciju sa sekvencijalnim brojevima tokom pregovora o algoritmu. Strict Key Exchange Countermeasures su novi sigurnosni mehanizmi u OpenSSH-u koji osiguravaju da svi dijelovi pregovora u fazi razmjene ključeva budu kompletni, neoštećeni i validni, kako bi se spriječile manipulacije poput Terrapin napada.

• **Primer Koda (ako je primenljivo):** U zvaničnom izvještaju objavljen je fragment koda iz OpenSSH-a koji pokazuje da se kompletni sadržaj prvih `SSH_MSG_EXT_INFO` poruka ne provjerava, odnosno omogućava "prefix-truncation":

```
if (msg == SSH2_MSG_EXT_INFO) {
ssh_packet_set_protocol_flags();
 return;
}
```

Ovaj dio logike dovodi do situacije da je moguće presjeći dio poruke i natjerati klijenta i server da vjeruju da koriste različite sigurnosne opcije, čime se ostvaruje downgrade napad.

5. Preporuke za mitigaciju

• **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da**.** OpenSSH je izdao patch u verziji **OpenSSH 9.6** (objavljen 18. decembra 2023.) koji uvodi *strict key-exchange countermeasures* i sprječava manipulaciju sekvencijalnih brojeva tokom inicijalne SSH razmjene.

• **Mitigation Strategy:** Rješenje za ublažavanje ranjivosti CVE-2023-48795 sastoji se u nadogradnji i konfiguraciji SSH servisa kako bi se onemogućila upotreba ranjivih algoritama i omogućile jače kriptografske kontrole. Preporučeni koraci su:

- Ažurirati OpenSSH server na verziju 9.6 ili noviju, jer ova verzija uključuje zaštitne mjere protiv „prefix truncation“ napada i uvodi strožu validaciju u fazi razmjene ključeva (key exchange).
- Onemogućiti upotrebu ranjivih algoritama u konfiguraciji SSH servera (`/etc/ssh/sshd_config`) i/ili klijenta (`/etc/ssh/ssh_config`).
- Forsirati sigurnije algoritme u SSH konfiguraciji, kao što su:AES-128-GCM, AES-256-GCM (za šifrovanje) i Sntrup761x25519-SHA512 (za razmjenu ključeva).
- Verifikovati konfiguraciju korišćenjem alata za bezbjednosnu provjeru.

• **Alternativni fix (ukoliko ne postoji vendorski):** U slučaju da nije moguće izvršiti nadogradnju OpenSSH-a (npr. legacy sistemi), privremena mitigacija može uključivati:

- potpuno isključivanje ChaCha20-Poly1305 algoritma
- isključivanje CBC ETM varijanti
- forsiranje AES-GCM algoritma

Ovo ne uklanja ranjivost iz koda, ali sprječava poznate načine eksploatacije i značajno smanjuje mogućnost man-in-the-middle manipulacije.