# Vulnerability Assessment Report Template

**Ime i prezime:** Anastasija Savić
**Tim:** 3
**Datum:** 26.10.2024.
**Scan Tool:** Nessus (10.8.3)
**Test okruženje:** Metasploitable3

---

## 1. Enumeracija CVE-a

- **CVE ID:** CVE-2023-48795

- **Opis:** SSH Terrapin Prefix Truncation Weakness omogućava napadaču postavljanje *man-in-the-middle (MITM)* napada na SSH server. Ranjivost nastaje zbog slabe zaštite kod ChaCha20-Poly1305 i CBC sa Encrypt-then-MAC algoritama. Na ovaj način, napadaču se omogućava da zaobiđe proveru integriteta i smanji sigurnost konekcije.

  - **Servis**: SSH (Secure Shell)
  - **Port**: 22
  - **Protokol**: TCP

---

## 2. CVSS skor

- **CVSS skor (numerička vrednost):** 5.9

- **Vektor:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
  - **AV (Attack Vector)**: N (Network) – Ranjivost može da bude eksploatisana preko mreže
  - **AC (Attack Complexity)**: H (High) – Napad zahteva složene korake i kontrolu mrežnog saobraćaja
  - **PR (Privileges Required)**: N (None) – Napadaču nisu potrebna privilegovana prava za eksploataciju
  - **UI (User Interaction)**: N (None) – Eksploatacija ne zahteva interakciju sa korisnicima
  - **S (Scope)**: U (Unchanged) – Ranjivost ne proširuje nivo pristupa van pogođenog sistema
  - **C (Confidentiality)**: N (None) – Ne utiče na poverljivost podataka
  - **I (Integrity)**: H (High) – Eksploatacija može značajno ugroziti integritet podataka
  - **A (Availability)**: N (None) – Ne utiče na dostupnost

- **Opravdanje:**
  Ova ranjivost ima skor, koji predstavlja umeren rizik, jer između ostalog predstavlja scenarijo za koji je mala verovatnoća da će se desiti. Da bi se napad izveo potrebno je da napadač ima visoko tehničko znanje, kako bi bio u *"man-in-the-middle"* poziciji. Iako napadač može manipulisati podacima koji se prenose i izvršiti napade, ne može direktno da otkrije ili onemogućiti slanje podataka (može samo da ih modifikuje ili presretne tokom prenosa).

  Javno dostupni dokazi koncepta (Proof-of-Concept - PoC) za ovu ranjivost ukazuju na moguću eksploataciju, ali zbog složenosti vektora, korišćenje ovih skripti nije jednostavno i zahteva napredno tehničko znanje.

---

## 3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Ne postoji javno dostupan eksploit za ovu ranjivost. Međutim, postoje blogovi i git repozitorijumi koji prikazuju minimalan kod ili dokaz koncepta (PoC) koji analiziraju problem i načine na koje ranjivost može da bude zloupotrebljena. Jedan od njih se nalazi na sledećoj stranici https://github.com/RUB-NDS/Terrapin-Artifacts?tab=readme-ov-file.

- **Opis eksploita:** Eksploit za ovu ranjivost omogućava *man-in-the-middle (MITM)* napad kojim se ometa sigurnost SSH konekcije preko slabih enkripcionih algoritama. Konkretno na navedenom repozitoriju možemo da vidimo različite tehnike eksploita, kao i njihovi rezultati. Najbolji rezultati su dobijeni u okviru napada na *downgrade* ekstenzije. *Downgrade* napadi funkcionišu tako što se napadač postavlja kao MITM. To znači da može da presreće i menja poruke između klijenta i servera. Tokom napada, napadač prisiljava klijenta i server da koriste slabije šifrovanje, koje može biti lakše kompromitovati, umesto jačih verzija koje bi inače bile korišćene (*downgrade*). Na taj način napadač povećava ranjivost i omogućuje manipulaciju komunikacije.

- **Kod eksploita (ukoliko postoji):** Na repozitorijumu je ostavljena bash skripta koja omogućava reprodukciju napada na *downgrade* ekstenzije. Ova skripta pokreće više docker kontejnera koji simuliraju servere i klijente u svrhu testiranja. Eksploitacija se zasniva na načinu na koji se koristi PoC proxy. Napadač koristi proxy da prevari klijentada komunicira sa serverom koristeći slabiji kriptografski algoritam (npr. `aes128-cbc`). To može da omogući napadaču da presretne ili dešifruje komunikaciju između klijenta i servera, potencijalno otkrivajući osetljive podatke. Na slici je prikazan deo koda Ova funkcija omogućava da se izabere PoC varijanta i pokretanje docker kontejner sa odgovarajućim PoC okruženjem.

```
function select_and_run_poc_proxy {
  echo "[i] This script supports the following extension downgrade attack variants as PoC:"
  echo -e "\t1) ChaCha20-Poly1305"
  echo -e "\t2) CBC-EtM (Unknown)"
  echo -e "\t3) CBC-EtM (Ping)"
  read -p "[+] Please select PoC variant to test [1-3]: " POC_VARIANT

  case $POC_VARIANT in
    1)
      POC_VARIANT_NAME="ChaCha20-Poly1305"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-chacha20-poly1305" ;;
    2)
      POC_VARIANT_NAME="CBC-EtM (Unknown)"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-unknown" ;;
    3)
      if [[ $SERVER_IMPL -eq 2 ]]; then
        echo "[!] CBC-EtM (Ping) variant requires OpenSSH 9.5p1 as the server. Please re-run the script."
        exit 1
      fi
      POC_VARIANT_NAME="CBC-EtM (Ping)"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-ping" ;;
    *)
      echo "[!] Invalid selection, please re-run the script"
      exit 1 ;;
  esac
  echo "[+] Selected PoC variant: '$POC_VARIANT_NAME'"

  echo "[+] Starting extension downgrade attack proxy on port $POC_PORT. Connection will be proxied to 127.0.0.1:$SERVER_PORT"
  docker run -d \
    --network host \
    --name $POC_CONTAINER_NAME \
    $POC_IMAGE --proxy-port $POC_PORT --server-ip "127.0.0.1" --server-port $SERVER_PORT > /dev/null 2>&1
}
```

---

## 4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Ranjivost je uočena kod SSH klijenata i servera koji koriste ChaCha20-Poly1305 i CBC sa Encrypt-then-MAC algoritmima bez striktne provere razmene ključeva, kao što su OpenSSH, paramiko, PuTTY... Lista svih SSH klijenata i servera može da se pronađe na https://terrapin-attack.com/patches.html. Ranjivost je uvedena zbog nedostatka konfiguracija za protivmere razmene ključeva koje bi štitile od MITM napada.

  Ranjivost je detektovana u verziji 1.4 plugina, koja je prvi put objavljena 27.12.2023. Poslednja izmena plugina bila je 29.01.2024. godine.

- **Primer Koda (ako je primenljivo):** (nije dat kod, ali je objašnjeno šta je glavni krivac ranjivosti)

  Glavni krivac ove ranjivosti je korišćenje kriptografskih algoritama i metoda autentifikacije koje klijent i server podržavaju prilikom uspostavljanja komunikacije. Neke od mogućih ranjivosti u konfiguraciji su:

1. ChaCha20-Poly1305
2. Bilo koje aes(128|192|256)-cbc šifre koje koriste podrazumevane MAC-ove (ili bilo koji MAC koji koristi Encript-then-MAC, na primer – hmac-sha2-256-etm@openssh.com)

---

## 5. Preporuke za mitigaciju

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

- **Mitigation Strategy:** Ažuriranje SSH implementacije kako bi se podržala stroga razmena ključa (*strict key exchange*), na ovaj način bi se rešile potencijalne slabosti u procesu početnog povezivanja (*handshake*). Treba voditi računa o tome da i klijent i server SSH implementacije budu ažurirane na verzije koje podržavaju strogu razmenu ključa.

  1. konfiguracija SSH servera – treba otvoriti konfiguracioni fajl ssh servera i podesiti da koristi listu strogih ključeva.
     ```
     sudo nano /etc/ssh/sshd_config

     KexAlgorithms diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
     ```

  2. konfiguracija SSH klijenta – konfiguracija treba da bude takva da klijent i server koriste iste algoritme za razmenu ključeva.
     ```
     sudo nano /etc/ssh/ssh_config

     KexAlgorithms diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
     ```

  Neki od alata pomoću kog je moguće da se automatizuje ažuriranje SSH sistema su: **Ansible**,**Chef**, i **Puppet.**

  Slika predstavlja primer konfiguracionog fajla ukoliko se koristi Ansible alat.

  ```
  - name: Ensure strict key exchange is enabled in SSH
    lineinfile:
      path: /etc/ssh/sshd_config
      regexp: '^KexAlgorithms'
      line: 'KexAlgorithms diffie-hellman-group-exchange-sha256
      state: present
    notify: Restart SSH
  ```

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