Vulnerability Assessment Report Template

**Ime i prezime: Miloš Stojanović R2 29/2024  
Tim: Tim 10  
Datum: 30.10.2024.  
Scan Tool:** Nessus (10.8.3)  
**Test okruženje:** Metasploitable3

### **1. Enumeracija CVE-a**

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

Napadač može da ukloni proizvoljnu količinu paketa koji se šalju tokom handshake-a tako što prosledi određeni sequence number. Time može promeniti algoritam za autentifikaciju korisnika i podesiti da se koristi neki slabiji. OpenSSH je ranjiv zaključno sa verzijom 9.5. Da bi se napad izvršio, potreban je man-in-the-middle napadač kao i kombinacija ChaCha20-Poly1305 algoritma sa Encrypt-then-MAC.

### **2. CVSS skor**

* **CVSS skor (numerička vrednost): 5.9**
* **Vektor:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Attack vector: Network – Napadač nije primoran da bude fizički blizu sistemu, već ga može napasti preko mreže.

Attack complexity: High – Potrebno je da napadač zna kako funkcioniše SSH protokol kao i OpenSSH. Pored toga je potrebno da zna da manipuliše paketima i da zna koji sequnce number treba da postavi.

Privileges Required: None – Napadaču nije potrebna nikakva veza sa sistemom za vršenje napada. Sam napad ne zahteva nikakve privilegije.

User interaction: None – Da bi se napad izvršio, korisnik ne mora izvršiti nikakvu akciju.

Scope: Unchanged – Opseg ranjivosti se ne menja, odnosno, ograničen je na sistem na kome se vrši napad.

Confidentiality: None – Napadom se ne mogu ukrasti podaci.

Integrity: High – Integritet podataka se narušava menjanjem algoritma za autentifikaciju korisnika.

Availability: None – Napad ne može dovesti do nedostupnosti sistema.

* **Opravdanje:**

Da bi napad uspeo, napadač mora biti u man-in-the-middle poziciji pošto je potrebno da menja podatke između dva peer-a. To doprinosi malo nižoj oceni. Na ocenu utiče i to što je napad veće kompleksnosti kao i posebna kombinacija algoritama. Ono što doprinosi značaju napada je to što je ranjivost na nivou protokola pa postoji dosta implementacija koje su ranjive.

### **3. Dostupnost eksploita**

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

<https://terrapin-attack.com/TerrapinAttack.pdf>

* **Opis eksploita:**

Prilikom handshake-a kada server vraća odgovor klijentu, man-in-the-middle menja sadržaj odgovora tako što iz paketa ukloni deo koji nosi podatke o algoritmima. Time klijent ne dobija dobre podatke i narušava se integritet podataka.

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

<https://github.com/RUB-NDS/Terrapin-Artifacts/>

<https://github.com/RUB-NDS/Terrapin-Artifacts/blob/main/pocs/ext-downgrade/ext_downgrade_chacha20_poly1305.py>



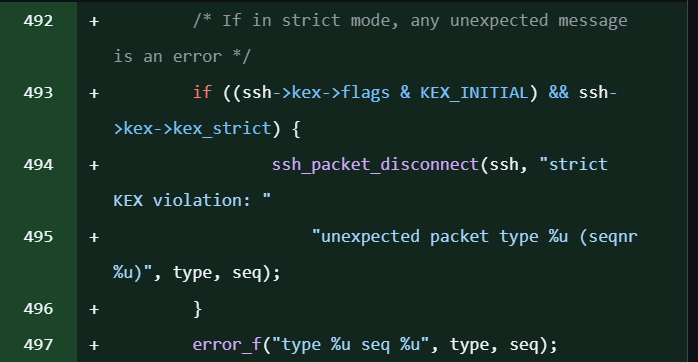
### **4. Analiza uzroka (root cause)**

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

Ranjivost postoji od prve verzije OpenSSH zaključno sa verzijom 9.5. Ranjivost je rešena u e7010dc komitu. Rešeno je tako što, ukoliko deo paketa ne odgovara konkretnom sequence number, handshake se prekida. Takođe, prvi paket mora da bude KEX\_INIT inače se handshake prekida.

[**https://github.com/PowerShell/openssh-portable/commit/e7010dc405279e32d26daf6b94134bf04761a4db**](https://github.com/PowerShell/openssh-portable/commit/e7010dc405279e32d26daf6b94134bf04761a4db)

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



### **5. Preporuke za mitigaciju**

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

Treba instalirati OpenSSH iznad verzije 9.5.

<https://github.com/PowerShell/Win32-OpenSSH/releases/tag/v9.5.0.0p1-Beta>

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

Treba zabraniti korišćenje slabijih algoritama, npr. chacha20-poly1305@openssh.com.