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-2016-2183 (SSL Medium Strength Cipher Suites Supported – SWEET32)

• **Opis:** Ova ranjivost, poznata kao **SWEET32**, odnosi se na upotrebu kriptografskih algoritama sa 64-bitnom veličinom bloka u TLS/SSL komunikaciji. Konkretno, nesigurnost proizlazi iz korištenja šifri kao što su 3DES (Triple-DES) u CBC (Cipher Block Chaining) režimu šifrovanja, što omogućava napadaču da izvrši tzv. ***birthday attack*** i potencijalno otkrije dio plaintext-a u toku dugotrajne enkriptovane sesije. U kontekstu okruženja koje je skenirano, Nessus je označio da udaljeni sistem podržava šifre srednje jačine i koristi 3DES-CBC(168) algoritam u okviru TLS sesija. Ranljivost pogađa SSL/TLS servise izložene na portovima 3389/tcp (RDP) i 443/tcp (HTTPS), što znači da napadač koji je pozicioniran na istoj mreži (Man-in-the-Middle scenario) može presresti saobraćaj i analizirati ponavljajuće blokove podataka, čime je omogućeno djelimično dešifrovanje informacija koje su prenesene u dužoj sesiji. Ranjivost je detektovana kroz Nessus plugin ID 42873, koji je klasifikovao ovaj problem kao High severity, pri čemu je naglašeno da je napad realističan u situacijama gdje se nalazi veliki protok enkriptovanih podataka (HTTPS pregledavanje, RDP sesije).

2. CVSS skor

• CVSS skor (numerička vrednost): 7.5 (High) - CVSS v3.0

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

- **AV:N (*Attack Vector:* Network):** Napad se sprovodi daljinski preko mreže, jer ranjivost pogađa SSL/TLS komunikaciju između klijenta i servera.

- **AC:L *(Attack Complexity:* Low):** Eksploatacija je niske složenosti, jer napadač samo mora imati pristup mrežnom saobraćaju između žrtve i servera (npr. na istoj Wi-Fi mreži).
- **PR:N (*Privileges Required:* None):** Nisu potrebne nikakve privilegije – napadač ne mora biti autentifikovan na sistemu.
- **UI:N (*User Interaction:* None):** Korisnik ne mora ništa da uradi – nema potrebe za klikovima, otvaranjem linkova ili interakcijom.
- **S:U (*Scope:* Unchanged):** Opseg ranjivosti je lokalizovan na jednu komponentu (TLS protokol) i ne utiče direktno na druge sisteme ili domene.
- **C:H (Confidentiality: High):** Povjerljivost podataka je ozbiljno ugrožena, jer napadač može rekonstruisati dijelove osjetljivih informacija iz HTTPS ili RDP sesija (npr. Set-Cookie, tokeni).
- **I:N (Integrity: None):** Integritet sistema nije direktno narušen – napadač ne može mijenjati sadržaj komunikacije.
- **A:N (*Availability:* None):** Dostupnost sistema nije pogođena, jer ranjivost ne izaziva pad servisa niti DoS.

• **Opravdanje:** Ova ranjivost ima CVSS skor 7.5, jer omogućava daljinsku dekriptaciju osjetljivih podataka bez privilegija i bez interakcije korisnika. Iako nije omogućeno potpuno preuzimanje sistema, uticaj na povjerljivost je značajan, naročito kada se prenose kolačići za sesiju, autentifikacioni tokeni ili druge poverljive informacije. Ranjivost je lako iskoristiva u uslovima gdje postoji produžena enkriptovana komunikacija (npr. duga HTTPS sesija ili RDP konekcija), što je čini ozbiljnom prijetnjom u realnim mrežnim okruženjima – posebno u Wi-Fi mrežama i mrežama sa slabom segmentacijom.

3. Dostupnost eksploita

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

• **Opis eksploita:** Za CVE-2016-2183 dostupne su javne implementacije napada SWEET32 koje demonstriraju mogućnost izvođenja tzv. *birthday* kriptoanalize nad 3DES šiframa korištenim u TLS/SSL sesijama. Eksploatacija funkcioniše tako što napadač generiše veliki broj zahtjeva prema serveru koristeći ranjivu cipher suite konfiguraciju (npr. 3DES-CBC), čime dolazi do ponavljanja blokova u CBC modu, što omogućava djelimičnu rekonstrukciju plaintext podataka (npr. HTTP cookies, session ID, tokeni). Eksploit funkcioniše pasivnim presretanjem saobraćaja (MITM), a zatim analizom ponavljanja 64-bitnih blokova nakon određenog broja iteracija. U praksi, eksploatacija zahtjeva veću količinu saobraćaja i dužu sesiju, ali je i dalje realno izvodljiva u mrežama gdje je napadač u stanju nadzirati promet (npr. Wi-Fi, lokalna LAN mreža). Napad je

praktično demonstriran od strane OpenSSL tima i istraživača sa https://sweet32.info, i postoji više proof-of-concept implementacija na GitHub-u i istraživačkim blogovima kripto zajednice.

• **Kod eksploita (ukoliko postoji):** Za CVE-2016-2183 postoje dostupni proof-of-concept (PoC) kodovi na GitHub-u i u okviru Sweet32 istraživačke publikacije. PoC skripte uglavnom koriste Python ili Ruby i automatizuju slanje velikog broja TLS zahtjeva prema serveru koji koristi 3DES-CBC cipher suite. Nakon prikupljanja dovoljne količine šifrovanog saobraćaja, skripta vrši statističku analizu enkriptovanih blokova, traži ponavljanje (birthday collision), te pokušava rekonstruisati dio plaintext-a (najčešće `Set-Cookie` vrijednosti ili druge sesijske tokene). Srž eksploita ne zasniva se na direktnom izvršavanju koda, već na kriptoanalizi i ponavljanju 64-bitnih blokova tokom dugotrajnog TLS session-a, nakon čega se vrši djelimično dešifrovanje. U tipičnoj implementaciji, PoC kontinuirano uspostavlja konekcije koristeći ranjivi 3DES cipher i vrši nadzor CBC blokova dok ne dođe do kolizije. Primjer pojednostavljenog principa eksploita:

```
while True:
  tls_session = request_to_server(cipher="3DES-CBC")
  observe_blocks(tls_session)
  detect_repeated_blocks()
  recover_plaintext_cookie()
```

Ovaj PoC predstavlja kriptografski side-channel napad, a ne direktnu RCE mogućnost. Kao posljedicu uspješne eksploatacije, napadač je u stanju da djelimično oporavi osjetljive podatke (npr. kolačiće sesije, identifikatore ili token-based autentifikaciju), naročito kod HTTPS i RDP protokola koji vrše duže enkriptovane sesije.

4. Analiza uzroka (root cause)

• **Uvođenje Greške (Commit/Verzija):** Ranjivost SWEET32 nije rezultat jedne greške u kodu, već posljedica dizajna kriptografskih algoritama sa 64-bitnom veličinom bloka (kao što su DES i 3DES) koji su originalno definisani još 1970-tih i 1990-tih godina (FIPS PUB 46). Iako 3DES funkcioniše kao trostruko šifrovanje DES-a, zadržana je blok veličina od samo 64 bita, što dovodi do tzv. *birthday collision* problema pri većoj količini podataka u CBC modu. U praktičnom smislu, ranjivost je postala aktuelna zbog činjenice da su brojni TLS/SSL servisi nastavili da podrazumijevano omogućavaju 3DES šifre u svojim OpenSSL, Java, Python, Node.js, Oracle, Cisco, Windows i drugim implementacijama. Tek krajem 2016. veliki vendor-i su počeli da uklanjaju 3DES iz “default cipher suite” konfiguracija. Dakle, uzrok nije specifična verzija jednog softvera,

već istorijsko nasleđe slabih šifara u kriptografiji, koje su ostale podržane iz kompatibilnosti i ranije standardizacije.

• **Primer Koda (ako je primenljivo):** Pošto je greška zasnovana na kriptografskom dizajnu, ne postoji konkretan "problematični red koda" kao kod klasičnih software bug-ova. Umjesto toga, ključni problem je upotreba 3DES šifre kao dio TLS handshake-a, što se u OpenSSL konfiguracijama manifestuje kroz cipher liste, npr: *TLS_RSA_WITH_3DES_EDE_CBC_SHA*. Odnosno, u konfiguracionim fajlovima se nalazio 3DES kao dozvoljeni (pa čak i prioritetni) cipher suite: *SSLv3, TLSv1: DES-CBC3-SHA*. Pošto je algoritam inherentno slab zbog 64-bitnih blokova, sama implementacija u OpenSSL nije "pogrešna", nego je problem u dizajniranoj kripto slabosti CBC moda sa malom blok veličinom.

5. Preporuke za mitigaciju

• **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Dobavljači softvera (npr. OpenSSL, Microsoft, Red Hat, Apache) su objavili ažuriranja i konfiguracione preporuke kojima se onemogućava upotreba slabih i srednje jakih šifara poput 3DES-CBC.

• **Mitigation Strategy:** Najefikasniji način mitigacije je onemogućavanje podrške za 3DES (Triple DES) u TLS konfiguraciji servera. Ovo se može uraditi:

- Izmjenom konfiguracije web servera (npr. `SSLProtocol` i `SSLCipherSuite` direktive u Apache/Nginx).
- Ažuriranjem OpenSSL biblioteke na verziju koja koristi sigurnije cipher suite-ove.

Na sistemima koji koriste RDP (kao što pokazuje port 3389 u skenu), preporučuje se konfiguracija grupnih politika da omoguće samo snažne šifre (npr. AES) i isključe TLS_RSA_WITH_3DES_EDE_CBC_SHA.

• **Alternativni fix (ukoliko ne postoji vendorski):** Ako nadogradnja nije moguća, preporučuje se sljedeće:

- Ručna izmjena cipher liste da se izostavi `3DES` (npr. u `openssl.cnf`, `sshd_config`, `nginx.conf`, itd.).
- Ograničiti trajanje TLS sesija kako bi se smanjila vjerovatnoća blok kolizije.
- Implementirati Application Layer mitigacije (npr. obavezna reautentikacija, rotacija kolačića).
- Postavljanje Web Application Firewall (WAF) koji prepoznaje i prekida sumnjive TLS tokove velikog volumena.