

Vulnerability Assessment Report Template

Ime i prezime: Ana Tamindzija

Tim: 5

Datum: 7.12.2025.

Scan Tool: Nessus (10.11.1)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-4000

- **Opis:**

Ranjivost poznata kao Logjam omogućava man-in-the-middle (MitM) napadaču da *snizi nivo bezbjednosti TLS konekcije* (downgrade attack) i primora strane u komunikaciji da koriste slab 512-bitni ili 1024-bitni Diffie-Hellman (DH) ključ, što omogućava presretanje i dešifrovanje saobraćaja.

Servisi pogođeni ranjivošću: ○ HTTPS (port 443, protokol TLS) ○

SMTP+StartTLS, IMAPS,

POP3S, IKEv1 VPN, SSH, itd.

Konkretno, u tvojoj skeniranju ranjivosti se pokazalo da:

- Server na IP adresi 192.168.56.101, port 443/tcp koristi:
 - TLS 1.0
 - Cipher: DHE_RSA_WITH_AES_128_CBC_SHA
 - DH MODP grupa: 1024-bit
 - Koristi poznatu (prethodno analiziranu) "Oakley Group 2", što Logjam napad čini još lakšim za izvršenje.

2. CVSS skor

- **CVSS v3.0 skor:** 3.7 (Nizak)

- **Vektor:**
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
- **Opravdanje:**
Zašto ova ranljivost ima dodeljen ovaj CVSS skor? Diskutujte o faktorima kao što su eksploataбилност, impact i obim ranljivosti.

Komponenta Vrijednost Značenje

AV:N	Network	Napad je moguć preko mreže (npr. Internet).
AC:H	High	Zahteva visok nivo vještina ili resursa (npr. državnog nivoa).
PR:N	None	Nisu potrebna posebna prava za izvršenje napada.
UI:N	None	Nije potrebna interakcija korisnika.
S:U	Unchanged	Nema uticaja na druge komponente sistema.
C:L	Low	Ograničen pristup povjerljivim podacima.
I:N	None	Nema uticaja na integritet.
A:N	None	Nema uticaja na dostupnost.

Opravdanje:

Skor je nizak jer:

- Eksploatacija zahtijeva visoke resurse (npr. priprema za napad nad poznatom 1024-bit grupom).
- Uticaj se uglavnom svodi na pasivno prisluškivanje (confidentiality).
- Nema direktnog oštećenja sistema (integritet/dostupnost nisu pogođeni).

3. Dostupnost eksploita

- **Postoji javno dostupan exploit (Da/Ne):**
Da.
Exploit za Logjam je opisan u tehničkom radu *"Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice"*, a proof-of-concept (PoC) alati i demonstracije su javno objavljeni od strane istraživačkog tima koji je otkrio ranljivost. Kôd je dostupan i na GitHub-u, iako izvođenje exploita zahtijeva značajne resurse (posebno za 1024-bitne grupe).
- **Opis exploita:**

Ako postoji exploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.

Logjam napad omogućava man-in-the-middle napadaču da:

- obori nivo sigurnosti TLS veze na 512-bitni *export-grade* Diffie-Hellman, ○ zatim računski razbije taj slab ključ, i ○ dešifruje ili modifikuje komunikaciju između klijenta i servera.

Exploit funkcioniše na sledeći način:

1. Napadač presreće početni TLS *ClientHello* paket.
2. Menja listu ponuđenih algoritama tako da server odabere DHE_EXPORT.
3. Kada server odgovori koristeći 512-bitni DH ključ, napadač može:
 - a. izračunati zajednički tajni ključ u roku od nekoliko minuta,
 - b. i dešifrovati celu komunikaciju.

Napad ne zahteva kompromitaciju bilo kog klijentskog uređaja – dovoljan je napad u mreži (npr. kao što može izvesti proxy, router, Wi-Fi AP ili ISP).

4. Analiza uzroka (root cause)

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

Logjam ranjivost nije posledica greške u kodu, već propusta u dizajnu TLS protokola i nasleđenih kriptografskih praksi iz 90-ih koje dozvoljavaju upotrebu slabih (export-grade) Diffie-Hellman grupa, prvenstveno zbog tadašnjih američkih zakona o izvozu kriptografije.

TLS verzije pogođene: TLS 1.0, 1.1 i delimično 1.2 (ako omogućavaju DHE_EXPORT)

Biblioteke pogođene: OpenSSL (do verzije 1.0.2), GnuTLS, NSS, itd.

Glavni uzrok: dozvola korišćenja slabih 512-bitnih DH grupa u TLS handshaku, što omogućava downgrade.

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

OpenSSL ranije dozvoljava DHE_EXPORT

```
/* Example from OpenSSL 1.0.x */
```

```
SSL_CTX_set_cipher_list(ctx, "ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH");
```

Ako nije eksplicitno zabranjeno EXP, server može ponuditi DHE_EXPORT ciphersuite.

5. Preporuke za mitigaciju

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

Da.

Svi relevantni vendori (OpenSSL, browseri, SSH) su zakrpili ranjivost još tokom 2015. godine.

- **Mitigation Strategy:**

Kako se konkretno apply-uje gore navedeni fix/patch, preporuka alata koji to može odraditi automatski...

1. **Onemogućiti DHE_EXPORT ciphersuites:**

- U OpenSSL konfiguraciji:

SSLProtocol all -SSLv2 -SSLv3 SSLCipherSuite

HIGH:!aNULL:!MD5:!EXP

2. **Koristiti DH grupe od najmanje 2048 bita:**

- Generisati grupu pomoću openssl dhparam -out dhparams.pem 2048

3. **Browser ažuriranja:**

- Chrome, Firefox, Safari, IE svi su onemogućili podršku za DHE_EXPORT u zadnjim verzijama 2015.

4. **Za SSH:**

- Update OpenSSH na verzije koje preferiraju ECDH (Elliptic Curve Diffie-Hellman).

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

Ako se ne može odmah primeniti vendor zakrpa:

- **Privremena mitigacija:** Ukloniti podršku za slabije kriptografske grupe u konfiguraciji ručno.
- **Alati za automatsku zaštitu:**
 - **testssl.sh** – skeniranje TLS konfiguracije
 - **Nessus**

- **SSL Labs** server test