Vulnerability Assessment Report Template

Ime i prezime: Marija Andrić
Tim: Kragujevac
Datum: 12.04.2025.godine
Scan Tool: Greenbone OS 24.10.6
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2017-16894

- **Opis:**
  Ova ranjivost pogađa Laravel framework (verzije do 5.5.21), gde .env fajl može biti direktno dostupan preko HTTP zahteva kada web server nije eksplicitno konfigurisan da blokira pristup skrivenim ili konfiguracionim fajlovima. Problem proizilazi iz previše permisivnih podrazumevanih dozvola prilikom kreiranja .env fajla, što omogućava neautorizovanim udaljenim napadačima pristup poverljivim konfiguracijama aplikacije (npr. kredencijali baze, API ključevi, mail server podaci). Lako ga je reprodukovati, sve što treba uraditi je posetiti *http://<target>/.env* i ako server nije zaštićen, sadržaj `.env` biće ispisan u plaintext formatu.

    - Servis: Web server (Apache/Nginx)
    - Port: 80/443
    - Protokol: HTTP/HTTPS

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 7.5
- **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
    - AV:N – Mrežni vektor napada
        - Napadač može biti bilo gde na internetu
        - Ne zahteva fizički pristup ili lokalnu mrežu
    - AC:L – Nizak nivo složenosti napada
        - Nema specijalnih uslova za uspešnu eksploataciju
    - PR:N – Ne zahteva privilegije
        - Napadač ne mora biti autentifikovan
    - UI:N – Ne zahteva interakciju korisnika

        - Ranjivost ne zahteva akciju od legitimnih korisnika
    - S:U – Utice samo na ugroženi sistem
        - Eksploatacija utiče samo na ugroženi komponent (Laravel aplikaciju)
    - C:H – Visok uticaj na poverljivost
        - Potpuni gubitak poverljivosti svih podataka u .env fajlu
        - Može dovesti do: otkrivanja baza podataka, API ključeva, mail konfiguracija...
    - I:N – Bez uticaja na integritet
        - Ranjivost ne omogućava modifikaciju podataka
    - A:N – Bez uticaja na dostupnost
        - Eksploatacija ne dovodí do DoS (Denial of Service)

- **Opravdanje:**
  Ranjivost ima visok CVSS zbog lakoće eksploatacije (neposredan HTTP zahtev) i visokog uticaja na poverljivost, jer se izlaganjem .env fajla otkrivaju osetljive konfiguracije, šifre, API ključevi i drugi podaci.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
  Postoje brojni javni dokazi o eksploataciji ove ranjivosti. Najrelevantniji među njima je u **Exploit-DB-u**, koji opisuje trivijalnu metodu pristupa `.env` fajlu putem jednostavnog HTTP GET zahteva. Ovo potvrđuje da je ranjivost lako reprodukovati i da se može eksploatisati bez posebnih alata ili naprednih tehnika.

    - *https://www.exploit-db.com/exploits/47129*

- **Opis eksploita:**
  Eksploit se sastoji od slanja jednostavnog HTTP GET zahteva ka putanji /.env na Laravel aplikaciji. Ukoliko fajl postoji i server dozvoljava čitanje, napadač može preuzeti ceo fajl. To može dovesti do otkrivanja baza podataka, mail konfiguracija, AWS ključeva, itd.
- **Kod eksploita (ukoliko postoji):**
  Primer jednostavnog URL poziva: bash curl http://metasploitable3.lan/.env

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost postoji u Laravel framework verzijama ispod 5.5.21 zbog funkcije writeNewEnvironmentFileWith u fajlu src/Illuminate/Foundation/Console/KeyGenerateCommand.php. Laravel se time oslanjao na podrazumevane permisije operativnog sistema, koje su u određenim okruženjima (npr. shared hosting) previše permisivne.

- **Primer Koda (ako je primenljivo):**
  U izvornom kodu u verzijama gde je postojao ovaj problem, permisije nisu bile eksplicitno postavljene: file_put_contents($this->environmentFilePath(), $contents);

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Suština problema sređena je u verziji 5.5.22 koja postavlja permisije .env fajla na 0600 (samo root korisnik može čitati/pisati). Zato se preporučuje ažuriranje Laravel framework-a na verziju 5.5.22 ili noviju.

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

  Ukoliko ažuriranje nije moguće, preporučuje se:

  - Ručno podešavanje permisija .env fajla.
  - Izmeniti konfiguraciju servera da odbija zahteve ka .env.

6. Izvori

- https://www.exploit-db.com
- https://www.cvedetails.com/cve/CVE-2017-16894/