Vulnerability Assessment Report Template

Ime i prezime: Aleksandar Sinđelić
Tim: Kragujevac
Datum: 10.12.2025
Scan Tool: OpenVAS (Greenbone OS 24.10.6)
Test okruženje: Metasploitable3

Apache mod_cgi ShellShock

1. Enumeracija CVE-a

- **CVE ID: CVE-2014-6271**

- **Opis:**
  Ovaj CVE je poznat kao ,,ShellShock". Ranjivost se nalazi u Shell-u i omogućava napadačima da izvršavaju komande. Ranjivost se dešava prilikom nepravilnog parsiranja varijabli okruženja. Da bi pristupili ovoj ranjivosti koristimo cgi skripte koje se nalaza na apach serveru

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8**
- **Vektor:** AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - **AV:N - Attack Vector (Network):** Napad se može izvesti udaljeno preko mreže, bez fizičkog pristupa.
  - **AC:L - Attack Complexity (Low):** Napad je jednostavan, bez posebnih uslova ili komplikacija.
  - **PR:N - Privileges Required (None):** Napadač ne treba nikakve prethodne privilegije ili korisnički nalog.
  - **UI:N - User Interaction (None):** Nije potrebna nikakva radnja korisnika da bi napad uspeo.
  - **S:U - Scope (Changed):** Ranjivost prelazi granice procesa.
  - **C:H - Confidentiality Impact (High):** Poverljive informacije mogu biti potpuno otkrivene.

    - **I:H – Integrity Impact (High):** Podaci i sistemske informacije mogu biti potpuno izmenjeni.
    - **A:H – Availability Impact (High):** Sistem ili usluga može biti potpuno onesposobljena.

- **Opravdanje:**
  Ocena je visok jer ova ranjivost omogućava napadaču da jednostavnim napadom preko mreže uzme potpunu kontrolu nad sistemom.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
  Exploit-db
- **Opis eksploita:**
  Eksploit koristi CGI skripte na web serverima koje koriste Bash za obradu zahteva. Napadač šalje HTTP zahtev sa malicioznom varijablom okoline u zaglavlju (npr. User-Agent ili Cookie), koja sadrži definiciju funkcije i komandu za izvršenje. Uspešan napad omogućava izvršavanje proizvoljnih komandi na serveru.
- **Kod eksploita (ukoliko postoji):**
  curl -H "User-Agent: () { :; };echo; /bin/bash -c 'cat /etc/passwd'" http://target/cgi-bin/hello_world.sh

---

4. Analiza uzroka (root cause)

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

  Uvedena je u verziji 1.14 i trajala je do verzije 4.3 zbog neadekvatne sanitizacije koda za parsiranje definisanih funkcija u varijablama okruženja.

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

Kada prosledimo neki header sa vrednosti: () { :; };echo; command; Možemo da dobijemo izlaz bilo koje komande koju izvršavamo, time možemo da pročitamo sve podatke.

---

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Može se rešiti tako što se instalira najnovija verzija Bash-a, odnosno verzija iznad 4.3.

Sensitive File Disclosure (HTTP)

1. Enumeracija CVE-a

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

- **Opis:**
  Ranjivost se nalazi u Laravel framework i ona omogućava napadaću da pristupi .env fajlu. Ovo je opasno jer taj fajl uglavnom sadrži poverljive informacije servera i baze.

2. CVSS skor

- **CVSS skor (numerička vrednost): 7.5**
- **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - **AV:N - Attack Vector (Network):** Napad se može izvesti udaljeno preko mreže, bez fizičkog pristupa.
  - **AC:L - Attack Complexity (Low):** Napad je jednostavan, bez posebnih uslova ili komplikacija.
  - **PR:N - Privileges Required (None):** Napadač ne treba nikakve prethodne privilegije ili korisnički nalog.
  - **UI:N - User Interaction (None):** Nije potrebna nikakva radnja korisnika da bi napad uspeo.
  - **S:U - Scope (Unchanged):** Ranjivost utiče samo na isti sigurnosni domen i ne prelazi granice procesa.
  - **C:H - Confidentiality Impact (High):** Poverljive informacije mogu biti potpuno otkrivene.
  - **I:H - Integrity Impact (High):** Podaci i sistemske informacije mogu biti potpuno izmenjeni.
  - **A:H - Availability Impact (High):** Sistem ili usluga može biti potpuno onesposobljena.

- **Opravdanje:**
  Ocena je visoka jer bilo ko sa pristupom mreži može da ukrade informacije iz .env fajla.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
- **Opis eksploita:**
  Napadač može jednostavno da poseti željeni sajt sa putanjom /.env. Ukoliko aplikacije nije dobro konfigurisana, napadač će moći da pristupi fajlu.
- **Kod eksploita (ukoliko postoji):**
  curl https://<target_site>/.env

4. Analiza uzroka (root cause)

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

  Ranjivost postoji od nastanka Laravela, sve do verzije 5.5.21. Funkcija writeNewEnvironmentFileWith u KeyGenerateCommand.php koristi file_put_contents bez provere restriktivnih dozvola.

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

5. Preporuke za mitigaciju

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

  1. Nadogradnja verzije laravela na 5.5.21 ili višu
  2. Konfiguracija servera da blokira pristup .env