# Vulnerability Assessment Report Template

**Ime i prezime: Danilo Cvijetic**
**Tim:**
**Datum: 22.11.2025**
**Scan Tool:** Nessus (10.10.1 (#10) LINUX)
**Test okruženje:** Metasploitable3

---

## 1. Enumeracija CVE-a

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

- **Opis:** Ova ranjivost, poznata kao Shellshock, pogađa GNU bash shell na Linux/Unix sistemima. Ranjivost omogućava napadaču da daljinski izvrši proizvoljan kod (Remote Code Execution - RCE) ubacivanjem zlonamjernih komandi u varijable okruženja.
  U kontekstu Metasploitable3 okruženja, ranjivost se najčešće eksploatiše preko HTTP servisa (Apache mod_cgi). Kada web server proslijedi HTTP zaglavlja (poput User-Agent) Bash-u kao varijable okruženja, Bash greškom izvršava kod koji se nalazi nakon definicije funkcije, dajući napadaču kontrolu nad serverom sa privilegijama web servisa (npr. www-data).

---

## 2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8 (Critical) CVSS 3.1**
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - AV:N (Network): Napad se izvodi daljinski preko mreže (npr. slanjem HTTP zahtjeva).
  - AC:L (Low Complexity): Eksploatacija je trivijalna, ne zahtijeva složene uslove niti "race conditions".
  - PR:N (None): Napadaču nisu potrebne nikakve privilegije niti nalog na sistemu.
  - UI:N (None): Nije potrebna interakcija korisnika (žrtve) da bi napad uspio.

- S:U (Unchanged): Ranjivost pogađa sam osnove sistema (Bash), ali ne mora nužno "skočiti" na druge sisteme (iako omogućava potpunu kontrolu tog hosta).
- C:H (High): Potpuni gubitak povjerljivosti (napadač može čitati bilo koji fajl dostupan korisniku servisa).
- I:H (High): Potpuni gubitak integriteta (napadač može mijenjati fajlove).
- A:H (High): Potpuni gubitak dostupnosti (napadač može obrisati fajlove ili srušiti server).

- **Opravdanje:**
  Ovo je jedna od najkritičnijih ranjivosti ikada otkrivenih jer pogađa osnovnu komponentu većine Linux sistema (Bash). Omogućava potpuno preuzimanje kontrole nad serverom bez autentifikacije, jednostavnim slanjem modifikovanog web zahtijeva. Impact je maksimalan jer omogućava RCE (Remote Code Execution).

---

## 3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  DA
- **Opis eksploita:**
  Postoje hiljade javno dostupnih skripti i modula (uključujući Metasploit modul exploit/multi/http/apache_mod_cgi_bash_env_exec) koji automatizuju ovaj napad. Eksploit funkcioniše tako što manipuliše formatom varijable okruženja. Napadač definiše praznu funkciju () { :;}; nakon koje odmah dodaje zlonamernu komandu. Bash verzije pre 4.3 ne staju sa parsiranjem nakon funkcije, već nastavljaju i izvršavaju ubačenu komandu..
- **Kod eksploita (ukoliko postoji):**
  komanda koja demonstrira ponašanje: env X='() { :;}; <komanda>' bash -c "<nešto>".

---

## 4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Greška postoji u izvornom kodu GNU Bash-a još od verzije 1.03 (iz 1989. godine), ali je otkrivena tek 2014. u verziji 4.3.

- **Primer Koda (ako je primenljivo):**
  Ranjivost se nalazila u fajlu variables.c u funkciji initialize_shell_variables. Kod je proveravao da li varijabla počinje sa () {, i ako da, prosleđivao je ceo sadržaj varijable funkciji parse_and_execute. Nedostatak validacije se ogledao u tome što parser nije bio

ograničen da učita samo definiciju funkcije, već je nastavljao da izvršava (execute) bilo koji kod koji je napadač dopisao nakon zatvaranja funkcije

Kada je ranjivost prijavljena odmah su usledile ispravke (prvobitni patch je bio nepotpun i naknadno su izdati dodatni patch-evi za povezane slabosti i drugi povezani CVE-ovi). Vendor-i su izbacili patch i ažuriranja za svoje pakete (distributionske zakrpe za bash paket).

---

## 5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Zakrpe za bash su objavljene od strane GNU projekta i distribuirane kroz Linux/Unix dobavljače (paketi za Ubuntu, Debian, RHEL, CentOS, OS X itd.).
- **Mitigation Strategy:**
  Ažuriranje verzije bash paketa. Ovo se može uraditi preko package manager-a vezanog za konkretni operativni sistem.

- **Alternativni fix (ukoliko ne postoji vendorski):**
  Ograničiti izloženost servisa koji mogu da exportuju promjenljive okruženja (npr. onemogućiti ili ograničiti CGI, provjeriti web aplikacije koje pozivaju shell).

  Upotreba web application firewall (WAF) za filtriranje sumnjivih HTTP header-a i inputa koji bi mogli prenositi zlonamerne promjenljive okruženja.