Vulnerability Assessment Report Template

Ime i prezime: Ana Tamindzija
Tim:
Datum: 7.12.2025.
Scan Tool: Nessus (10.11.1)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**
  Naziv ranjivosti: ShellShock – *Bash Remote Code Excecution*

  Opis ranjivosti:

  Ranjivost omogućava daljinsko izvršavanje proizvoljnog koda na sistemima koji koriste ranjive verzije GNU Bash komandnog interpretera (verzije do 4.3). Problem nastaje zbog toga što Bash nepravilno obrađuje stringove nakon definicije funkcije u promenljivama okruženja. Napadač može iskoristiti ovo tako što kreira posebno oblikovanu (malicioznu) promenljivu okruženja koja uključuje dodatne komande nakon funkcije – i te komande se izvršavaju.

  Eksploatacija je moguća gdje god korisnik ili napadač ima mogućnost da postavi promjenljive okruženja koje Bash koristi. Shellshock ranjivost se može eksploatisati kroz više vektora. U okviru Metasploitable3 okruženja, ranjivost Shellshock se najčešće eksploatiše putem HTTP servisa, odnosno preko Apache web servera koji koristi modul za CGI skripte (mod_cgi).
  Kada web server obradi HTTP zahtjev, određena zaglavlja – poput User-Agent – mogu biti proslijeđena kao promjenljive okruženja CGI skripti koje se izvršavaju u Bash-u.
  Ako je sistem ranjiv, Bash će pogrešno interpretirati sadržaj zaglavlja koje sadrži definiciju funkcije, te će izvršiti svaki dodatni kod koji slijedi nakon nje.
  Na taj način, napadač može izvršiti proizvoljne komande na sistemu, najčešće sa privilegijama korisnika web servera (npr. www-data), čime se stiče kontrola nad kompromitovanim servisom. U kontekstu Nessus-a, ranjivost je eksploatisana putem SSH sesije, gdje je preko promjenljive TERM injektovan maliciozni kod koji je Bash izvršio.

---

2. CVSS skor

- **CVSS skor (v3.0): 9.8 (Critical)**
- **Vektor:**
  AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Komponenta	Značenje
AV:N	*Attack Vector: Network* – Napad se može izvršiti preko mreže.
AC:L	*Attack Complexity: Low* – Eksploatacija ne zahtijeva posebne uslove.
PR:N	*Privileges Required: None* – Napadač ne treba privilegije.
UI:N	*User Interaction: None* – Nije potreban korisnikov input.
S:U	*Scope: Unchanged* – Napad ne utiče na druge komponente van cilja.
C:H	*Confidentiality: High* – Omogućava pristup svim podacima.
I:H	*Integrity: High* – Može menjati ili brisati podatke.
A:H	*Availability: High* – Može onesposobiti sistem.

- **Opravdanje:**
  Ova ranjivost dobija visok (kritičan) skor jer je **eksploatacija izuzetno laka (AC:L)** – dovoljno je samo da napadač pošalje posebno formatiranu promenljivu okruženja. **Ne zahtijeva privilegije (PR:N)** – napad je moguć i od strane neautentifikovanog korisnika. **Nije potrebna interakcija korisnika (UI:N)** – što povećava automatizaciju i opasnost. **Uticaj je ogroman (C:H, I:H, A:H)** – napadač može pristupiti, promeniti ili uništiti podatke, pa čak i preuzeti potpunu kontrolu nad sistemom. **Eksploatacija postoji (public exploit)** – dostupna je kroz Metasploit, Core Impact i druge alate. Klasifikovana je kao „known exploited“ (poznato iskorišćena). **Vulnerabilnost je stara ali još uvijek se pronalazi na sistemima** koji nisu ažurirani, kao što je slučaj sa starim verzijama Debian 7.0. Ranjivost je postala **kritična** tek sa širenjem mrežnih servisa (kao što su CGI skripte u Apache-u i udaljeni pristupi putem SSH-a) koji automatski prosljeđuju korisnički kontrolisane vrijednosti (npr. User-Agent, TERM) kao promjenljive okruženja Bash-u.

---

3. Dostupnost eksploita

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

- **Opis eksploita:**
  Eksploit se zasniva na manipulaciji načina na koji Bash parsira promjenljive okruženja. U ranjivim verzijama, Bash greškom **nastavlja da interpretira sve što se nalazi nakon definicije funkcije** i automatski izvršava tu komandu. Tipičan payload definiše **praznu funkciju**, a zatim odmah nakon nje dodaje komandni dio koji će biti izvršen:
  () { :; }; <zlonamjerna_komanda>
- **Kod eksploita (ukoliko postoji):**
  Najjednostavniji PoC izgleda ovako: env X='() { :;}; /usr/bin/id' bash -c "echo test"

  U kontekstu Metasploitable3, ranjivost je skenirana putem Nessus-a, koji je iskoristio varijablu TERM poslatu tokom SSH inicijalizacije, i ubacio komandu: () { :;}; /usr/bin/id > /tmp/nessus.xxxxxx

---

4. Analiza uzroka (root cause)

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

  Ranjivost potiče iz greške u komandnom interpreteru GNU Bash, koja je prisutna još od verzije 1.03(iz 1989. godine), iako je otkrivena tek 2014.godine, kada je bila prisutna u verziji 4.3.

  Zbog načina na koji je Bash rukovao funkcijama definisanim putem promjenljivih okruženja, Bash parsira varijable okruženja koje sadrže funkcijsku sintaksu (npr. () {}), i poziva funkciju parse_and_execute nad kompletnim sadržajem varijable. U ranijim verzijama nije postojao mehanizam za validaciju da li nakon funkcije slijedi dodatni, potencijalno maliciozni kod.

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

  Ranjivi dio se nalazio u fajlu variables.c, u funkciji initialize_shell_variables(). Ova funkcija je prepoznavala vrijednosti u formatu () { ... } kao funkcije, ali nije provjeravala da li sadržaj nakon zatvaranja funkcije sadrži dodatne komande – te su one automatski izvršavane.

---

5. Preporuke za mitigaciju

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

  Da. Nakon što je ranjivost prijavljena u septembru 2014. godine, zvanični razvojni tim GNU Bash-a je objavio seriju bezbjednosnih zakrpa, počevši od Bash verzije 4.3 patch 26, koje adresiraju i CVE-2014-6271 i kasnije otkrivene povezane ranjivosti (CVE-2014-7169 i druge).

Linux distribucije kao što su Debian, Ubuntu, Red Hat, CentOS, i druge su objavile ažurirane verzije bash paketa putem svojih package manager-a.

- **Mitigation Strategy:**
  Najpreporučljiviji način je ažuriranje verzije Bash paketa. Na većini sistema ažuriranje se vrši standardnim sistemskim alatima, npr. Debian/Ubuntu: sudo apt update; sudo apt install --only-upgrade bash. Ovim se instalira verzija Bash-a u kojoj su zakrpljene sve poznate ranjivosti vezane za ShellShock.

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

  Može se privremeno deaktivirati pokretanje Bash-a za servise koji prosljedjuju varijable okruženja. Moguće privremene mjere: zamijeniti Bash drugim shell-om(npr. dash, sh, zsh) za CGI skripte u Apache-u, ograničiti pristup CGI skriptama, ukloniti mod_cgi iz Apache konfiguracije ako nije potreban. Instalacija i pravilna konfiguracija Web Application Firewall-a (npr. ModSecurity, AWS WAF, Cloudflare WAF) može efikasno filtrirati sumnjive HTTP zaglavlja i zahtjeve, uključujući manipulaciju User-Agent, Referer i sličnih polja koja se često koriste kao vektor za ubacivanje zlonamjernih promjenljivih okruženja. Ova mjera ne zamjenjuje patch, ali značajno smanjuje šanse za uspješnu eksploataciju.