Vulnerability Assessment Report Template

Ime i prezime: Miloš Stojanović R2 29/2024
Tim: Tim 10
Datum: 30.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**

  Bash podržava export-ovanje shell funkcija kao environment variables. Ranjivost je to što bash nastavlja da parsira i izvršava shell komande nakon definisanja funkcije. Na primer:

  EXAMPLE=() { … }; some-command

  Ako se ovakva funkcija export-uje, kada se bude uvela kao environment variable u neki drugi bash proces, komanda posle definicije, tj. some-command će se izvršiti. Ovim se dozvoljava remote arbitrary code execution. Ranjivost je prisutna u GNU Bash do verzije 4.3.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8**
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

  Attack vector: Network – Napadač nije primoran da bude fizički blizu sistemu, već ga može napasti preko mreže.
  Attack complexity: Low – Napadaču nije potrebno mnogo znanja za izvođenje napada. Takođe, sam napad nije previše kompleksan, jer je samo potrebno posle definicije funkcije proslediti niz komandi koje treba izvršiti.

Privileges Required: None – Napadaču nije potrebna nikakva veza sa sistemom za vršenje napada. Sam napad ne zahteva nikakve privilegije (možda komande budu zahtevale). Korisnik ne mora biti autentifikovan niti autorizovan da bi izvršio napad.
User interaction: None – Da bi se napad izvršio, korisnik ne mora izvršiti nikakvu akciju.
Scope: Unchanged – Opseg ranjivosti se ne menja, odnosno, ograničen je na sistem na kome se vrši napad.
Confidentiality: High – Napadom je moguće ukrasti podatke pa se time narušava poverljivost podataka.
Integrity: High – Napadač može izvrsiti komandu kojom je moguće izmeniti ili obrisati podatke pa bi se time narušio i integritet podataka.
Availability: High – Zbog toga što je komanda koja se injektuje proizvoljna, može doći i do narušavanja dostupnosti sistema.

- **Opravdanje:**

  Ovim napadom je moguće izvršiti proizvoljni kod na nekom sistemu. Podešavanje environment varijabli nije teško uraditi, a i najčešće ne postoji mehanizam kojim bi se to sprečilo pa je zbog toga ovaj napad lako izvesti. Sam opus stvari koje može uraditi napadač injektovanjem komande je veliki, od krađe podataka do narušavanja dostupnosti sistema, pa zato ovaj napad ima visoku ocenu. Jos jedna stavka koja pridodaje značaju napada je to što nije potrebna nikakva akcija korisnika da bi se on izvršio, što znači da se napad može izvršiti u skoro svakom trenutku i da bi možda bio težak za uočavanje.

---

3. Dostupnost eksploita

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

  https://www.exploit-db.com/exploits/34766

- **Opis eksploita:**
  Exploit iskorišćava to što CGI (common gateway interface, koji služi kao veza interfejs između web servera i eksternih programa (CGI skripti)) smešta HTTP zaglavlja u environment variables kada prosleđuje vrednosti u Bash. Kada se u nekom zaglavlju nalazi maliciozna komanda, ona dolazi do Bash-a kao environment varijabla i kada se ta varijabla bude koristila, ta komanda će se izvršiti.

- **Kod eksploita (ukoliko postoji):**

```php
$context = stream_context_create(
    array(
        'http' => array(
            'method'  => 'GET',
            'header'  => 'User-Agent: () { :;}; /bin/bash -c "'.$cmd.'"'
        )
    )
);
```

---

4. Analiza uzroka (root cause)

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

  Ranjivost postoji od prve verzije Bash-a sve do verzije 4.3 kada je uveden fix. Greška je bila u tome sto je nakon definicije funkcije nastavljano izvršavanje komandi.

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

  https://ftp.gnu.org/pub/gnu/bash/bash-4.3-patches/bash43-025

---

5. Preporuke za mitigaciju

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

  Treba instalirati Bash počevši sa verzijom 4.3. Proveru da li je sistem ranjiv na ovu ranjivost i update je moguće uraditi komandom:

  env x='() { :;}; echo vulnerable' bash -c 'echo hello' | grep vulnerable && (sudo apt-get update && sudo apt-get install bash) || echo 'not vulnerable'

  https://gist.github.com/charlespeach/b83939eb4495c6118767

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