Vulnerability Assessment Report Template

Ime i prezime: Hristina Adamović R2 20/2024
Tim: 2
Datum: 27.10.2024.
Scan Tool: Nessus 10.8.3
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2020-14567

- **Opis:**
  Ranjivost u MySQL Server proizvodu kompanije Oracle (komponenta: Server: Replikacija). Pogođene verzije su 5.7.29 i ranije, kao i 8.0.19 i ranije. Ova lako eksploatabilna ranjivost omogućava visoko privilegovanom napadaču sa mrežnim pristupom putem više protokola da kompromituje MySQL Server. Uspešna eksploatacija ove ranjivosti može dovesti do toga da napadač izazove blokiranje (hang) ili česti pad servera (kompletan DoS - Denial of Service).

    - **Servis**: MySQL Server (komponenta za replikaciju)

    - **Port**: 3306 (standardni MySQL port, može varirati)

    - **Protokol**: TCP/IP, može koristiti više protokola u zavisnosti od konfiguracije replikacije

---

2. CVSS skor

- **CVSS skor (numerička vrijednost): 4.9 (srednja)**

- **Vektor:**
  AV = Attack Vector: Network - napad može biti izvršen preko mreže.

  AC = Attack Complexity: Low - ovaj napad ne zahtijeva mnogo tehničkog znanja, lako ga je izvesti.

PR = Privileges Required: High - napadač mora imati visoke privilegije, poput administratorskog ili root pristupa.

UI = User Interaction: None - napad se može izvršiti bez interakcije korisnika.

S = Scope: Unchanged - opseg ranjivosti nije promijenjen.

C = Confidentiality Impact: None - nema uticaja na povjerljivost.

I = Integrity Impact: None - nema uticaja na integritet.

A = Availability Impact: High - ugrožava dostupnost sistema, napadač može učiniti neke usluge nedostupnim.

- **Opravdanje:**
  CVSS skor je srednji jer ranjivost zahtijeva visoke privilegije za napadača, što smanjuje rizik u poređenju sa ranjivostima koje zahtijevaju niske ili nikakve privilegije. Ranjivost se može izvesti bez korisničke interakcije i rezultat uspješnog napada je potpuni gubitak dostupnosti MySQL servera, te to povećava skor. Nedostatak uticaja na poverljivost i integritet podataka doprinosi tome da CVSS skor ostane srednji.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Ne.
- **Opis eksploita:**
  Trenutno ne postoji javno dostupna verzija eksploita za ovu ranjivost. Eksploatacija bi mogla uključivati korištenje specifičnih zahtjeva unutar replikacionog okruženja MySQL servera, izazivajući prekid u radu servera zbog grešaka u kodu za rukovanje replikacijom. Posljedice uspješnog napada uključuju pad MySQL servera, čime se ugrožava dostupnost podataka za sve povezane aplikacije.

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

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost je prisutna u MySQL verzijama 5.7.29 i ranije i 8.0.19 i ranije. Detalji o tačnom uvođenju greške nisu poznati javnosti, ali se odnose na problematično rukovanje replikacionim komandama u bazi podataka, što uzrokuje DoS.

- **Primer Koda (ako je primenljivo):**
  Nema dostupnog koda za detaljan uvid u uzrok greške.

---

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Oracle je objavio zakrpu za ovu ranjivost u bezbjednosnom ažuriranju iz jula 2020. Preporučuje se ažuriranje MySQL servera na verzije iznad 5.7.29 i 8.0.19 gdje je ranjivost ispravljena. Primjenu ažuriranja mogu olakšati alatke kao što su yum update za Red Hat ili apt-get upgrade za Ubuntu distribucije.

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

  Ako ažuriranje nije odmah dostupno, preporučuje se ograničavanje pristupa replikacionim funkcijama samo na provjerene korisnike sa visokim nivoom privilegija i praćenje servera zbog potencijalnih znakova nestabilnosti ili DoS napada.