Vulnerability Assessment Report Template

Ime i prezime: Teodor Vidaković
Tim:
Datum: 20.11.2025.
Scan Tool: Nessus (10.10.1 (#10) LINUX)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**
  Ova ranjivost pogađa MySQL Server (komponenta: Server: Replication) u verzijama 5.7.29 i niže, kao i 8.0.19 i niže. Ranjivost omogućava napadaču sa visokim privilegijama i mrežnim pristupom da daljinski izvrši napad na server koristeći više mrežnih protokola. Najčešće pogođeni port je 3306 i protokol TCP. Uspešan napad može dovesti do pada ili zamrzavanja MySQL servera, čime se gubi dostupnost servisa (DoS napad). Nije moguće preko ove ranjivosti kompromitovati poverljivost ili integritet podataka.

  Link

2. CVSS skor

- **CVSS skor (numerička vrednost): 4.9 (Base Score)**
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
  - **AV:N** (Attack Vector: Network): Napad se izvodi preko mreže, nije potreban lokalni pristup.
  - **AC:L** (Attack Complexity: Low): Potreban je minimalan napor za uspešan napad. Ne zahteva posebno predzanje ili uslove.
  - **PR:H** (Privileges Required: High): Napadač mora imati visoke privilegije na servisu.
  - **UI:N** (User interaction: None): Nije potrebna interakcija korisnika.
  - **S:U** (Scope: Unchanged): Napad ne utiče na druge komponente van MySQL servera.
  - **C:N** (Confidentiality: None): Nema uticaja na poverljivost. Podaci korisnika ostaju neotkriveni.
  - **I:N** (Integrity: None): Nema uticaja na integritet. Podaci ostaju nepromenjeni.

    - **A:H** (Availability: High): Kompletna ili kontinuirana nedostupnost servisa.
- **Opravdanje:**
  Skor je srednje vrednosti 4.9 jer napadač mora imati visoke privilegije, ali je napad vrlo jednostavan i može potpuno onesposobiti servis (DoS). Nije moguć “remote code execution” ili krađa podataka, samo DoS. Ova ranjivost može dovesti do nedostupnosti baze podataka, što direktno utiče na rad aplikacija koje se oslanjaju na nju. Neke od mogućih posledica su:

    - Privremeni prekid poslovnih operacija i servisa koje zavise od MySQL-a.
    - Mogući gubitak prihoda zbog nedostupnosti usluga.
    - Potencijalno narušavanje reputacije organizacije usled neplaniranog zastoja.
    - Rizik dodatnih troškova za saniranje incidenta i vraćanje sistema u funkcionalno stanje.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Ne**
- **Opis eksploita:**
  Do sada nije objavljen javni exploit kod. Eksploatacija se bazira na zloupotrebi replikacionog protokola ili posebnih mrežnih zahteva, ali zbog potrebe za visokim privilegijama ova ranjivost nije u širokoj upotrebi.
- **Kod eksploita (ukoliko postoji):**
  Nema javnog primera koda za direktan eksploit. Objavljen je vendor patch pre same distribucije eksploita.

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Greška je prisutna u Oracle MySQL Replication komponenti u verzijama 8.0.19 i nižim i 5.7.29 i nižim zbog neadekvatnog rukovanja određenim replikacionim zahtevima. Kada se ti zahtevi izvrše nepropisno ili u neodgovarajućem redosledu, mogu srušiti MySQL server.

- **Primer Koda (ako je primenljivo):**
  Nije javno objavljen tačan kod, ali osnovni problem je u funkcijama koje obrađuju određene replikacione komande u MySQL serveru. Patch je primenjen u commitima za verzije 8.0.20 i 5.7.30.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
    - Ažurirati MySQL server na verziju 8.0.20 ili 5.7.30 ili noviju. Oracle Critical Patch koji mitiguje ovaj CVE: https://www.oracle.com/security-alerts/cpujul2020.html
    - Za Ubuntu:
        - Mysql-8.0 verzija 8.0.20-0ubuntu0.20.04.1
        - Mysql-5.7 verzija 5.7.30-0ubuntu0.18.04.1
    - Pre update-a preporučuje se backup podataka i testiranje na rezervnom sistemu.
    - Nije preporučeno onemogućavanje servisa na produkciji kao workaround.

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

  Nema efektivnog workaround-a osim patcha. Kratkoročno se može ograničiti lokalni pristup MySQL serveru na proverene adrese pomoću firewall pravila, ali ovo ne eliminiše ranjivost korisnika sa visokim privilegijama.