Vulnerability Assessment Report Template

MySQL Authentication Bypass

**Ime i prezime: Jovana Jelić  
Tim:  
Datum:12/11/2024  
Scan Tool:** Nessus (10.0.1)  
**Test okruženje:** Metasploitable3

Sve korake ispod treba ponoviti za svaku ranjivost

### **1. Enumeracija CVE-a**

* **CVE ID: CVE-2012-2122**
* **Opis:**Ukratko upišite ranjivost i način na koji ona pogađa servis. Dajte detaljne informacije o servisu (npr., ime servisa, port, protokol…).
* Ovu ranjivost sam identifikovala putem Nessus skeniranja na MySQL portu (3306). Nessus prepoznaje ovu grešku u autentifikaciji i prijavljuje je kao ozbiljnu ranjivost.
* Platforma: MySQL baze podataka
* Verzije MySQL servera od 5.1 do 5.5.19, postoji greška gde napadaci imaju mogucnost prijave bez ispravne lozinke. Zbog načina na koji MySQL validira lozinku, moguće je da napadač ponavlja prijavu koristeći proizvoljne lozinke dok server greškom ne prihvati nevalidnu lozinku kao ispravnu, tada server omogućava pristup kao root korisnik što znači da napadač može izvršavati bilo koje SQL upite, kao sto su I čitanje, modifikacija ili brisanje podataka.
* MySQL verzija koja je prisutna na Metasploitable3 omogućava napadačima da se prijave bez validne lozinke. Ranjivost se dešava zbog greške u verifikaciji lozinke, koristeci neuspesne pokusaje gde MySQL greškom prihvata bilo koju lozinku nakon više pokušaja, pruzajuci konkretnom napadaču da pristupi bazi podataka. MySQL servis je dostupan na portu 3306.

### **2. CVSS skor**

* **CVSS skor (numerička vrednost): 10.0**
* **Vektor: AV/AC/PR/UI/S/C/I/A**Opišite vektor string (npr. AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) opišite svaku pojedinačnu komponentu.
* AV (Attack Vector): N (Network): Eksploatacija se može izvršiti preko mreže.
* AC (Attack Complexity): L (Low): Napadač jednostavno koristi netačnu lozinku i nastavlja da pokušava dok ne uspe.
* PR (Privileges Required): N (None): Nisu potrebne prethodne privilegije.
* UI (User Interaction): N (None): Eksploatacija se odvija bez interakcije korisnika.
* S (Scope): U (Unchanged): Eksploatacija nema uticaj na druge sisteme.
* C (Confidentiality): H (High): Napadač može pristupiti podacima u bazi.
* I (Integrity): H (High): Napadač može menjati ili brisati podatke u bazi.
* A (Availability): H (High): Napadač može značajno ugroziti dostupnost baze podataka.
* **Opravdanje:**Zašto ova ranljivost ima dodeljen ovaj CVSS skor? Diskutujte o faktorima kao što su eksploatabilnost, impact i obim ranljivosti.
* Ranljivost pruza direktan pristup bez lozinke, što kompromituje sve aspekte sigurnosti konkretnog sistema.

### **3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne):** DAIzvršite pretragu (npr. Exploit-DB, GitHub, blog postovi) za javno dostupan eksploit koji je vezan za ovaj CVE.

**Javno dostupan eksploat:**

* **Exploit-DB:** Exploit-DB 19091 - Exploit demonstrira način na koji napadač može da koristi ovu ranjivost da zaobiđe autentifikaciju.
* **GitHub:** Primeri eksploita dostupni su i na GitHub-u kao deo demonstracija i deo istraživačkih skripti.
* **Opis eksploita:**Ako postoji eksploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.

Eksploatacija uključuje upisivanje netačne lozinke više puta dok server ne prihvati prijavu. Na taj način, napadač dobija pristup bazi kao root korisnik.

* **Kod eksploita (ukoliko postoji):**Objasnite srž eksploita, dajte screenshot koda (samo glavni dio)

# Jednostavno ponavljanje prijave dok ne uspe

mysql -u root -p

# Ponovite unos lozinke (prazan string ili netačna lozinka) više puta dok server ne prihvati prijavu

### **4. Analiza uzroka (root cause)**

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

Istražite kako je ranljivost uvedena. Identifikujte verziju, tačan commit, ili biblioteku koja je izazvala ranljivost (npr. "Uvedeno u verziji X zbog neadekvatne validacije u biblioteci Y").

Greška u kodu MySQL verzije 5.1.x do 5.4.x koja neadekvatno obrađuje proveru lozinke.

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

Pružite primer koda koji je glavni krivac, ako je dostupan.

### **5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da (ispravljeno u novijim verzijama)
* **Mitigation Strategy:**Kako se konkretno apply-uje gore navedeni fix/patch, preporuka alata koji to može odraditi automatski…

Update-ovati MySQL server na najnoviju verziju koja ispravlja ovu ranjivost.

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

Opis kako bi se ovo moglo rešiti dobudživanjem trenutne verzije

Konfigurisati firewall tako da ograniči pristup MySQL portu (3306) samo na autorizovane IP adrese dok se ne izvrši azuriranje.