UNIVERSITAS GADJAH MADA

Client Report – MySQL Authentication Bypass (CVE-2012-2122)

Company: Penelitian Damas 2024
Authors: N.R. Rosyid, Y. M. Saputra, Anni K. Fauziyah, Yoan Navie Ananda
Date: 28 August 2025
Version 1.0

1. Executive Summary

This report provides the results of a security assessment conducted on the mysql service running on host 10.33.102.225. The system was identified to be running mysql version MySQL 5.5.23, which is affected by a known critical authentication bypass vulnerability (CVE-2012-2122). The vulnerability allows unauthenticated attackers to gain root access to the mysql service without knowing the correct password.

2. Vulnerability Overview – CVE-2012-2122

CVE ID: CVE-2012-2122
Tipe: Authentication Bypass
CVSS v2: 7.5 (High)
Description:
A logic flaw in MySQL's authentication mechanism allows an attacker to login with an incorrect password under certain conditions. Specifically, due to the way the memcmp() function processes authentication hashes, invalid passwords have a 1 in 256 chance of being accepted.

Affected Versions:
- MySQL < 5.1.63
- MySQL < 5.5.24
- MariaDB < 5.5.23

References:
- https://nvd.nist.gov/vuln/detail/CVE-2012-2122
- https://www.exploit-db.com/exploits/19091

3. Assessment Approach

The assessment involved:
Phase 1 – Scanning:
Service discovery and fingerprinting using Nmap tool:
nmap -sV -sC -Pn -O -oN nmap_results.txt 10.33.102.225

Phase 2 – Enumeration:
Version enumeration of the MySQL service.

Phase 3 – Version Analysis:
Validation of vulnerability presence based on known affected verseions

Phase 4 – Exploitation:
Proof-o-Concept (PoC) exploitation to confirm unauthorized access and send SQL Command SHOW DATABASES;

Tools used include Nmap and a custom brute-force script for CVE-2012-2122 verification.

4. Key Findings

Upon successful exploitation, the following databases were enumerated: information _schema, mysql, performance_schema, test.

Target Host	10.33.102.225
Open Port	3306/tcp
Service	mysql
Detected Version	MySQL 5.5.23
Vulnerability Status	Confirmed Exploitable
Login Attempt Count	409 attempts before successful login

5. Analysis

The target was identified as running mysql version MySQL 5.5.23, which matches the list of vulnerable versions for CVE-2012-2122. Exploitation results show that an attacker can gain root access through random brute-force attempts, without a valid password, and successfully execute SQL commands.

6. Risk Impact

An attacker who successfully exploits this vulnerability can gain administrative access to the database system. This can result in:
- Unauthorized access and modification of sensitive data.
- Lateral movement within the internal network.
- System compromise and data exfiltration.

Given the ease of exploitation and potential damage, this vulnerability is classified as High Risk.

7. Recommendatioins and Conclution

To mitigate this vulnerability, we recommend the following actions:
1. Immediately upgrade mysql to version MySQL 5.5.23 or later:
   - MySQL ≥ 5.5.24
   - MariaDB ≥ 5.5.24
2. Restrict remote access to mysql (port 3306) to trusted IP addresses only.
3. Enable detailed logging and monitor for unusual access patterns.
4. Implementation firewall or fail2ban for blocking brute-force login attempts.
5. Posibly implement socket authentitation (unix_socket) in local system.

The presence of CVE-2012-2122 on the MySQL service of the assessed host poses a significant

security risk. Timely patching and access control measures are essential to prevent unauthorized access and data breaches.

8. Referensi Teknis

- CVE-2012-2122 – https://nvd.nist.gov/vuln/detail/CVE-2012-2122
- Exploit PoC – https://www.exploit-db.com/exploits/19091
- Oracle Patch Note – https://www.oracle.com/security-alerts/cpujul2012.html