CVE-2016-6662

Oracle MySQL Vulnerability

MySQL adalah software untuk mengelola database yang bersifat open source. Dawid Golunski menemukan celah pada versi MySQL 5.5.52, 5.6.x – 5.6.33 dan 5.7.x – 5.7.15 yang memungkinkan user lokal untuk membuat konfigurasi sewenang-wenang dan melewati mekanisme perlindungan yang ada dengan menyetting file general_log_file ke konfigurasi my.cnf. Celah ini dapat dimanfaatkan melalui serangan SQL injection atau penyerang yang mempunyai hak mengelola database tersebut baik secara lokal maupun secara web melalui PhpMyAdmin. Bila penyerangan berhasil, penyerang dapat mengeksekusi kode semaunya dengan hak akses root sehingga penyerang dapat membahayakan database yang sedang berjalan.

Konsep penyerangan terbagi menjadi 3 yaitu :

1. Menyuntik konfigurasi jahat yang dibuat penyerang ke dalam file konfigurasi MySQL yang ada pada sistem yang mempunyai hak akses yang lemah.
2. Membuat file konfigurasi baru pada data direktori MySQL.
3. Penyerang mendapatkan hak akses SELECT/FILE untuk mengakses ke fungsi logging yang mana fungsi ini hanya dimiliki oleh admin MySQL. Kemudian penyerang dapat menambah dan memodifikasi konfigurasi pada MySQL.

Simulasi penyerangan.

Sebagai admin sistem pada target

1. Membuat sebuah database percobaan dan mengatur hak aksesnya :

   ```
   CREATE DATABASE pocdb;
   GRANT FILE ON *.* TO 'attacker'@'%' IDENTIFIED BY 'p0cpass!';
   GRANT SELECT, INSERT, CREATE ON `pocdb`.* TO 'attacker'@'%';
   ```

2. Simulasikan write access pada file konfigurasi mysql yang ada.

   ```
   [isamchk]
   key_buffer      = 16M

   For example, /etc/mysql/my.cnf on Debian:

   # chown mysql:mysql /etc/mysql/my.cnf

   # ls -l /etc/mysql/my.cnf
   -rw-r--r-- 1 mysql mysql 3534 Sep 11 02:15 /etc/mysql/my.cnf
   ```

3. Mulai ekploitasi sebagai penyerang dan restart mysql jika proses ekploitasi selesai.

Sebagai penyerang

1. Masuk ke lokasi library pada mysql_hookandroot_lib.c
2. Jalankan script yang dibuat dengan format ./namascript -dbuser attacker -dbpass 'p0cpass!' -dbhost 192.168.1.10 -dbname pocdb -mycnf /etc/mysql/my.cnf.

Analisa hole

Mysql sangat berguna dalam pengelolaan database. Dari penjelasan diatas akan sangat berbahaya ketika orang lain dapat menambahkan atau mengubah database yang kita miliki. Sehingga kita perlu mengamankan database kita dari serangan, baik serangan dari luar maupun serangan dari dalam. Untuk memperbaiki hole ini dengan cara mengupdate mysql server kita ke versi yang lebih baru.

Source script:
https://github.com/jivoi/pentest/blob/master/exploit_nix/mysql_rce_cve_2016_6662/mysql_rce_cve_2016_6662.txt