УДК 004.65

Колгін Володимир Андрійович, студент гр. 125м-16-1,
Науковий керівник: Начовний І.І., ст. викладач кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ОБХІД АУТЕНТИФІКАЦІЇ СУБД MARIADB ТА MYSQL ЧЕРЕЗ «CVE-2012-2122»

Ця стаття дає ознайомитися з вразливістю CVE-2012-2122, яка була знайдена в СУБД MariaDB та MySQL, що дозволяє обійти механізм аутентифікації.
Ключові слова – MariaDB, MySQL, memcmp (), glibc, аутентифікація.

ВСТУП

Фахівці з інформаційної безпеки проекту MariaDB надали детальні відомості про серйозну уразливість в популярній СУБД MySQL, а також в СУБД MariaDB, яка ділить з MySQL загальну технологічну базу. В MySQL вразливість отримала номер CVE-2012-2122.

В офіційних заявах розробників спочатку наводилося дуже мало даних про усунення вразливості, що було зроблено навмисно, щоб не провокувати інтерес хакерів. Коли значна частина користувачів MySQL і MariaDB отримали досить часу для обновлення, розробники MariaDB заявили про виявлення в СУБД MySQL досить простий в використання критичної уразливості CVE-2012-2122, що дозволяє обійти авторизацію і отримати доступ до вмісту БД.

ПРИЧИНА ВИНИКНЕННЯ ВРАЗЛИВОСТІ

Вразливим виявився модуль "sql / password.c", в якому для повернення результату порівняння хеш пароля застосовується функція "memcmp ()". Наявність уразливості залежить не тільки від версії СУБД, але і від компілятора, за допомогою якого була проведена збірка. Так, популярні компілятори (gcc і BSD libc) і оригінальні дистрибутиви мають безпечну реалізацію вразливою функції "memcmp ()", що робить систему невразливою для виявленої помилки. У разі, якщо значення, що повертається функцією "memcmp ()" не піддається додатковій перевірці, зловмисникові достатньо здійснити близько 300 спроб авторизації з відомим ім’ям користувача (наприклад, "root") і випадковими значеннями пароля для отримання доступу до СУБД.

Суть в тому, що при підключенні користувача MariaDB / MySQL обчислюється токен (SHA від пароля і хеша), який порівнюється з очікуваним значенням. При цьому функція memcmp () повинна повертати значення в діапазоні -128..127, але на деяких платформах (в glibc в Linux з оптимізацією під SSE) повертаєме значення може випадати з діапазону. У підсумку, в 1 випадку з 256 процедура порівняння хеша з очікуваним значенням завжди повертає значення true, незалежно від хеша. Іншими словами, система вразлива перед випадковим паролем з ймовірністю 1/256. [1]

Проста команда на bash дає зловмисникові рутовий доступ до уразливому сервера MySQL, навіть якщо він не знає пароль.

$ For i in `seq 1 1000`; do mysql -u root --password = bad -h 127.0.0.1 2> / dev / null; done

mysql> [2]

УМОВИ АТАКИ

Уразливість CVE-2012-2122 може бути проексплуатовано тільки в тому випадку, якщо продукт встановлений на системі, яка дозволяє функції memcmp () повертати значення за межами діапазону від -128 до 127. Серед таких систем можна відзначити

Linux платформи, які використовують SSE-оптимізований glibc (бібліотека GNU C). Бінарні версії MySQL, які поширюються виробником, уразливості не схильні. Якщо MySQL працює на системі даного типу, код, який порівнює криптографічний хеш введеного користувачем пароля з хешем, розміщеним в базі даних для конкретної облікового запису, буде здійснювати аутентифікацію навіть в разі надання некоректного пароля. Імовірність спрацьовування даної проломи, якщо продукт відповідає зазначеним вище вимогам, становить 1 до 256. [3]

МОЖЛИВІ ЗБИТКИ

Після успішної експлуатації уразливості модуль копіює таблицю користувачів сервера бази даних, яка містить всі хеші паролів. Зловмисник може згодом зламати хеші паролів і надалі отримувати неавторизований доступ до сервера навіть після усунення вразливості.[3]

ЯК ЗАХИСТИТИСЯ

Уразливими виявилися всі версії MySQL і MariaDB до версії 5.1.61, 5.2.11, 5.3.5, 5.5.22 включно. Перелік операційних систем, на які поширюється дана уразливість:

- Ubuntu Linux 64-бит (10.04, 10.10, 11.04, 11.10, 12.04);
- OpenSuSE 12.1 64-бит MySQL 5.5.23-log;
- Нестабильная ветка Debian 64-бит MySQL 5.5.23-2;
- Fedora;
- Arch Linux.

ВИСНОВКИ

Будьте обачливими, навіть те програмне забезпечення, якому Ви повністю довіряєте, може бути вразливим. Ніколи не довіряйте користувачу, бо він є потенційним зловмисником. Частини програмного забезпечення були самостійними і не вразливими і тільки коли вони об’єдналися з’явилася вразливість. Ці речі неможливо передбачити, але це не означає, що ми не повинні реагувати та вирішувати поставленні перед нами цілі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стаття: Обхід авторизації (Електрон. ресурс) / Спосіб доступу: URL: http://sitesco.ru/thread-11627.html

2. Стаття: Вразливість MySQL під Ubuntu 64-bit (Електрон. ресурс) / Спосіб доступу: URL: https://rdot.org/forum/archive/index.php/t-2218.html.

3. Доклад: Вразливість MySQL (Електрон. ресурс) / Спосіб доступу: URL: https://www.securitylab.ru/news/425688.php