

## Doomsday Engine - Bug #1003

### [Hexen] SEGV during 3D weapon use

2012-03-05 10:45 - vvv1

<b>Status:</b> Closed	<b>Start date:</b> 2012-03-05
<b>Priority:</b> High	<b>% Done:</b> 100%
<b>Assignee:</b> skyjake	
<b>Category:</b>	
<b>Target version:</b> 1.9.8 Unstable	
<b>Description</b> Using 3D weapon near walls causes segmentation fault.  How to reproduce:  1. Copy Axe 3D model from <a href="http://colocall.net/~vvv/HUD-Axe.pk3">http://colocall.net/~vvv/HUD-Axe.pk3</a> to data/jhexen/auto directory. The model is extracted from XCCP 1.2. 2. Unpack files from attached savegame.zip to runtime/hexndata/hexen directory. 3. Start Hexen. 4. Load the game named "Segmentation fault". 5. Use the weapon (press Ctrl or left mouse button).  <b>Labels:</b> jHexen	

#### History

##### #1 - 2012-03-05 10:45 - skyjake

The crash was caused by null pointer access. Some of the particles created by the "lightning" hit effect didn't have a current sector set, presumably because they were being spawned outside the map.

##### #2 - 2012-03-10 10:59 - vvv1

The patch from git does not fix SEGV. The bug can be reproduced as described in the first message.

##### #3 - 2012-03-10 16:12 - skyjake

Some offline comments:

-----

This assert fails in P\_NewParticle():

```
pt->sector = R_PointInSubsector(FIX2FLT, FIX2FLT)->sector;  
assert(pt->sector);
```

dani: Hmm, this would indeed suggest a degenerate nodebuild case. I'll test this once I've merged the map-cache changes (I've addressed the two causes of degenerates known to me).

##### #4 - 2012-03-12 10:09 - vvv1

#### Attachments:

- [http://sourceforge.net/p/deng/bugs/\\_discuss/thread/b8af9a2d/b784/attachment/savegame.zip](http://sourceforge.net/p/deng/bugs/_discuss/thread/b8af9a2d/b784/attachment/savegame.zip)

##### #5 - 2012-03-12 11:38 - dani

The underlying issue (that of a degenerate subsector) has been fixed for Monday's build451.

##### #6 - 2012-03-25 00:28 - dani

Reopening this issue as this failure case has returned some time after build 451.

I currently suspect this is caused by a bool to boolean conversion somewhere in the BSP node builder as this problem only resurfaced when the boolean type definition changed.

##### #7 - 2012-04-13 14:18 - skyjake

Checked it out in a debugger: a particle with a NULL sector is being processed in linkGeneratorParticles().

There is now an assert() to catch this in Generators\_LinkToList().

**#8 - 2012-04-20 13:36 - danij**

I think the best we can hope to achieve with this issue at present is to quietly kill any particle which ends up in a degenerate BSP leaf (i.e., sector == NULL as per the assert() in Generators\_LinkToList() ).

This particular instance can be resolved but there are many others. The Hexen IWAD is (unfortunately) so riddled with mapping bugs that solving all the degenerate cases is a very tall order indeed.

**#9 - 2012-04-20 17:24 - skyjake**

Pushed a fix that omits all particles in a NULL sector from rendering.