Doomsday Engine - Bug #330

Crash bug in jdoom with 3d models enabled

2006-08-05 02:30 - ashridah

Status:	Closed	**Start date:**	2006-08-05
Priority:	Urgent	**% Done:**	100%
Assignee:			
Category:			
Target version:	1.9.0-beta4		

Description

I'm getting the following crash (repeatable for me)
in map 6 of doom2. This occurs seemingly randomly in
other maps, but once it starts happening, it happens
consistently at some point in the level.

If 3d models are turned off, the crash doesn't
happen.
The following is a backtrace of SVN head:

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 4155610800 (LWP 18307)]
0x080b2203 in PG_InitForNewFrame ()

at /home/ashridah/deng/doomsday/engine/portable/src/rend_particle.c:246
246                 if(gen->ptcs[k].stage >= 0)
(gdb) bt
#0  0x080b2203 in PG_InitForNewFrame ()

at /home/ashridah/deng/doomsday/engine/portable/src/rend_particle.c:246
#1  0x080e1fbf in R_RenderPlayerView
(player=0x81e9b20)

at /home/ashridah/deng/doomsday/engine/portable/src/r_main.c:586
#2  0xf6e3ed9e in D_Display ()

at /home/ashridah/deng/doomsday/plugins/jdoom/src/d_refresh.c:302
#3  0x0807d05e in DD_DrawAndBlit ()

at /home/ashridah/deng/doomsday/engine/portable/src/dd_loop.c:177
#4  0x0807d445 in DD_GameLoop ()

at /home/ashridah/deng/doomsday/engine/portable/src/dd_loop.c:142
#5  0x08075e82 in DD_Main ()

at /home/ashridah/deng/doomsday/engine/portable/src/dd_main.c:600
#6  0x080f672a in main (argc=7, argv=0xffea07b4)

at /home/ashridah/deng/doomsday/engine/unix/src/dd_uinit.c:303
(gdb) print k
$1 = 0
(gdb) print gen
$2 = (ptcgen_t *) 0xf5ef16fe
(gdb) print gen->ptcs
$3 = (particle_t *) 0x1af405e
(gdb) print gen->ptcs[0]
Cannot access memory at address 0x1af405e
```

At this particular point, it looks like several
entries in active_ptcgens are corrupted. pointers
like 0x1af405e are not valid.

Attached is my jdoom config and a save game file from

the level that's causing the crash (it happens at some point during the level). Also attaching a doomsday -v -v output for references to addon packs

Labels: Graphics

History

#1 - 2006-08-05 02:31 - ashridah

doomsday -v -v output

Attachments:

- http://sourceforge.net/p/deng/bugs/_discuss/thread/690a26cc/cfe0/attachment/doomsday.out

#2 - 2006-08-05 02:31 - ashridah

savegame from level 6

Attachments:

- http://sourceforge.net/p/deng/bugs/_discuss/thread/690a26cc/572f/attachment/DoomSav0.dsg

#3 - 2006-08-05 02:32 - ashridah

Attachments:

- http://sourceforge.net/p/deng/bugs/_discuss/thread/690a26cc/90c3/attachment/jdoom.cfg

#4 - 2006-08-07 13:10 - ashridah

Logged In: YES
user_id=2918

http://www.icculus.org/~ashridah/core.8628.bz2 <-- core dump from crashed doomsday instance.

http://www.icculus.org/~ashridah/doomsdaycomp.tar.gz <-- compressed tree of compiled doomsday executable in case symbols don't match up.

Compiled i386 executables probably expects tree to be /home/ashridah/tree/[bin|lib|share]/ I suspect.

#5 - 2006-08-29 10:43 - danij

Logged In: YES
user_id=849456

I have had further users confirm this problem. One was under windows.

It looks like this might be the cause of the obscure seg faults when using jDRP.

#6 - 2006-09-06 16:42 - skyjake

(originally posted by anonymous SF.net user)

Logged In: YES
user_id=734315

I get similar segfaults, those times I traced it, it was in the same statement that caused the fault in this report. However, I only get them when I have particle effects enabled. I can't reproduce the error with 3d-models enabled and particle effects disabled, but do get segfaults when 3d-models are disabled and particle effects enabled (but less frequently). Level 10 in doom 2 is horrible to try and play through without disabling all neat effects.

It does seem to happen more often when flying demons are involved, i.e., caco-demons, lost souls etc.

I'm running Linux (debian) and have just about all
jfiles-packages installed.

#7 - 2010-04-05 14:15 - danij

Please recheck this in 1.9.0-Beta6.9 (when released), as a rare zone heap corruption issue was found and fixed; this very well may have been the cause.