Doomsday Engine - Bug #887

[x64 Ubuntu] Crash when loading a level

2010-04-08 08:24 - kurikai

Status:	Closed		**Start date:**	2010-04-08
Priority:	Normal		**% Done:**	100%
Assignee:				
Category:				
Target version:	1.9.0-beta6			

Description

In the new doomsday Engine release 1.9.0-beta6.9
Running in Ubuntu 10.04 beta-1 64bit
after doomsday loads, go through the menu to load the first map of DOOM2 and it crashes sometime after selecting the difficulty
got a gdb backtrace and the output from the terminal.
http://pastebin.com/8tbuDiRs
http://pastebin.com/rDE8DRAu

History

#1 - 2010-04-18 04:21 - skyjake

(originally posted by anonymous SF.net user)

I installed Kees karmic(9.10) 32bit build on my lucid(10.04) 64bit install.
And no crashes happen, so I am leaning towards a problem with the newer version of gcc

#2 - 2010-04-29 04:49 - skyjake

(originally posted by anonymous SF.net user)

Installing Kees lucid(10.04) 32bit build on my lucid(10.04) 64bit install.
It crashes while in the level. I think it could be a problem with rendering something, cause I went to an area and it keeps crashing at the same spot, ubt I can move around other areas of the level with no problem

I will have to test it with the 9.10 build as I didn't go to the area with that installed build

I'm using the shareware wad to test right now
It crashes first level up the stairs to the left at the start of the level when you turn around to head back down the stairs

#3 - 2010-04-29 04:56 - yagisan

At kurikai's request I'm having a look into this bug. Currently basing my testing on branch 1.9.0-beta6 with a head of 8b6fb49d4cfbd89253f4e0e4f8ecc77be03ed52a using doom2.wad and no jpacks

Ubuntu Karmic i386 GCC 4.4 - Release Build: No Crash
Ubuntu Karmic i386 GCC 3.3 - Release Build: No Crash
Ubuntu Karmic i386 ICC 11.1.046 - Release Build: No Crash.

As I get time I'll give it a test on my 64bit Karmic machines, and possibly a lucid VM.

Regards,
Yagisan

#4 - 2010-05-03 01:01 - yagisan

Ubuntu Karmic amd64 GCC 4.4 - Release Build: No Crash

I think it's time to find out what Lucid is doing differently.

#5 - 2010-05-03 01:14 - skyjake

(originally posted by anonymous SF.net user)

with lucid 64bit build using beta6 branch with a head of 0dce956169680211e1c202f4dc436e99baf15146
gcc version 4.4.3 (Ubuntu 4.4.3-4ubuntu5)
I was able to play through the first map of doom1.wad before a crash
here is the gdb http://pastebin.com/CukkC1xd
using doom2.wad it crashed sometime between choosing the difficulty and the first level starting

here is the gdb http://pastebin.com/CMeYmnmk

#6 - 2010-05-03 08:37 - yagisan

Ubuntu Lucid amd64 GCC 4.4 - Release Build: Crash
Ubuntu Lucid amd64 GCC 4.4 - Debug Build: No Crash

It is interesting to note that under Ubuntu Lucid, every single release from 1.9.0-beta6.0 through to current git head will crash at the same point when built as a release build. This strongly hints that something is being mis-compiled. I'll investigate the RelWithDebInfo mode and alternative compilers when I have time.

#7 - 2010-05-05 11:18 - danij

Great detective work yagisan, I had suspected this was a compiler-specific issue. It may be the automatic vectorize support gcc enables that is the cause as makovic found here: http://sourceforge.net/tracker/?func=detail&aid=2995576&group_id=74815&atid=542101

#8 - 2010-05-05 11:24 - yagisan

Ubuntu Lucid amd64 GCC 4.4 - Release Build: Crash
Ubuntu Lucid amd64 GCC 4.4 - RelWithDebInfo Build: No Crash
Ubuntu Lucid amd64 GCC 4.3 - Release Build: No Crash
Ubuntu Lucid amd64 LLVM Clang - Release Build: No Crash
Ubuntu Lucid amd64 GCC 4.4 - RelWithDebInfo Build + -ftree-vectorizer: Crash

This conclusively demonstrates that Doomsday is being affected by a mis-compile relating to -ftree-vectorizer in GCC 4.4 - my current suggestion would be to try that suggested patch and/or change the default build to RelWithDebInfo to work around this bug.

Regards,
Yagisan