Doomsday Engine - Bug #2052

[OS X] Crash when loading a map (clang, release build)

2015-05-14 22:47 - skyjake

Status:	Closed	**Start date:**	2015-05-14
Priority:	Urgent	**% Done:**	100%
Assignee:	Deng Team		
Category:	Defect		
Target version:			

Description

Build 1591, Apple LLVM version 6.1.0 (clang-602.0.49).

When running the client or doomsday-server, in map.cpp, sortLineOwners gets stuck in an infinite recursion. splitLineOwners returns null, and the recursion continues down the first argument of the mergeLineOwners call.

GCC and MSVC release builds work normally.

Associated revisions

Revision aee9fecd - 2015-05-15 20:20 - skyjake

Fixed|Client|Map|Clang: Crash in optimized build (undefined behavior)

During line owner sorting, LineOwner was returning references to null,
which is undefined behavior according to the C++ standard. The result
was that Clang's optimizer produced incorrect code.

http://stackoverflow.com/questions/2727834/c-standard-dereferencing-null-pointer-to-get-a-reference

IssueID #2052

History

#1 - 2015-05-14 22:48 - skyjake

- Tags changed from MapData, Server to MapData, Server, Mac

#2 - 2015-05-14 22:56 - skyjake

- Tags changed from MapData, Server, Mac to MapData, Server, Mac, Client

- Subject changed from [OS X] Server crashes when loading a map (clang) to [OS X] Crash when loading a map (clang)

- Description updated

#3 - 2015-05-14 22:56 - skyjake

- Description updated

#4 - 2015-05-14 23:02 - skyjake

- Subject changed from [OS X] Crash when loading a map (clang) to [OS X] Crash when loading a map (clang, release build)

#5 - 2015-05-15 14:15 - skyjake

- % Done changed from 0 to 50

After investigating closer, this looks a lot like an optimization bug in clang. (MSVC and GCC builds work fine.)

I'll just disable optimization on this part of the code when building with clang.

#6 - 2015-05-15 20:16 - skyjake

- Status changed from In Progress to Resolved

- % Done changed from 50 to 100

#7 - 2015-05-15 20:24 - skyjake

I dug a little deeper and found the root cause. (Which is nice because qmake doesn't easily support source file specific build options.)

#8 - 2015-05-15 21:49 - skyjake

- Status changed from Resolved to Closed

#9 - 2015-06-08 10:48 - skyjake

- Target version deleted (49)