

Doomsday Engine - Bug #2167

SIGSEGV during ~Subsector (e.g., ICARUS.WAD map01)

2016-07-22 08:26 - skyjake

Status:	Closed	Start date:	2016-07-22
Priority:	High	% Done:	100%
Assignee:	daniij		
Category:	Regression		
Target version:			

Description

It appears the recent changes in world data structures have introduced a SIGSEGV. I have seen an occasional crash with larger custom WADs, such as Icarus.

Thread 14 Crashed:: CallbackThread

```
0 0x000000010e514583 world::ConvexSubspace::bspLeaf() const +
35 (convexsubspace.cpp:194)
1 0x000000010e5a7670 world::Subsector::sector() + 176 (subsect
or.cpp:83)
2 0x000000010e5a7758 world::Subsector::plane(int) + 24 (subsec
tor.cpp:94)
3 0x000000010e0f87fa world::ClientSubsector::Impl::mappedPlane
(int) + 74 (clientsubsector.cpp:168)
4 0x000000010e0f86b3 world::ClientSubsector::Impl::map(int, wo
rld::ClientSubsector*, bool) + 115 (clientsubsector.cpp:211)
5 0x000000010e0f85d1 world::ClientSubsector::Impl::clearMappin
g(int) + 33 (clientsubsector.cpp:227)
6 0x000000010e0f7a17 world::ClientSubsector::Impl::subsectorBe
ingDeleted(world::Subsector const&) + 87 (clientsubsector.cpp:643)
7 0x000000010e5a74f6 world::Subsector::~~Subsector() + 182 (sub
sector.cpp:77)
8 0x000000010e107578 world::ClientSubsector::~~ClientSubsector(
) + 88 (clientsubsector.h:38)
9 0x000000010e0f7415 world::ClientSubsector::~~ClientSubsector(
) + 21 (clientsubsector.h:38)
10 0x000000010e0f7439 world::ClientSubsector::~~ClientSubsector(
) + 25 (clientsubsector.h:38)
11 0x000000010e116e81 void qDeleteAll<QList<Vertex*>::const_ite
rator>(QList<Vertex*>::const_iterator, QList<Vertex*>::const_iterator) + 81 (qalgorithms.h:318)
12 0x000000010e59c011 void qDeleteAll<Sector::Impl::Planes>(Sec
tor::Impl::Planes const&) + 65 (qalgorithms.h:326)
13 0x000000010e59bf98 Sector::Impl::Subsectors::~~Subsectors() +
24 (sector.cpp:122)
14 0x000000010e59ad55 Sector::Impl::Subsectors::~~Subsectors() +
21 (sector.cpp:122)
15 0x000000010e59c313 Sector::Impl::~~Impl() + 291 (sector.cpp:4
4)
16 0x000000010e59adb5 Sector::Impl::~~Impl() + 21 (sector.cpp:44
)
17 0x000000010e59add9 Sector::Impl::~~Impl() + 25 (sector.cpp:44
)
18 0x000000010e4d3858 de::PrivateAutoPtr<Sector::Impl>::reset(S
ector::Impl*) + 152 (libcore.h:397)
19 0x000000010e4d37a5 de::PrivateAutoPtr<Sector::Impl>::~~Privat
eAutoPtr() + 21 (libcore.h:387)
20 0x000000010e4d3785 de::PrivateAutoPtr<Sector::Impl>::~~Privat
eAutoPtr() + 21 (libcore.h:387)
21 0x000000010e4d36c1 Sector::~~Sector() + 49 (sector.h:49)
22 0x000000010e59a8f5 Sector::~~Sector() + 21 (sector.h:49)
23 0x000000010e59a919 Sector::~~Sector() + 25 (sector.h:49)
24 0x000000010e116e81 void qDeleteAll<QList<Vertex*>::const_ite
rator>(QList<Vertex*>::const_iterator, QList<Vertex*>::const_iterator) + 81 (qalgorithms.h:318)
```

```
25 0x000000010e116de6 void qDeleteAll<QList<Vertex*> >(QList<Vertex*> const&) + 54 (qalgorithms.h:326)
26 0x000000010e564256 world::Map::Impl::~Impl() + 390 (map.cpp:337)
27 0x000000010e563275 world::Map::Impl::~Impl() + 21 (map.cpp:355)
28 0x000000010e563299 world::Map::Impl::~Impl() + 25 (map.cpp:326)
29 0x000000010e572a38 de::PrivateAutoPtr<world::Map::Impl>::reset(world::Map::Impl*) + 152 (libcore.h:397)
30 0x000000010e572985 de::PrivateAutoPtr<world::Map::Impl>::~PrivateAutoPtr() + 21 (libcore.h:387)
31 0x000000010e572965 de::PrivateAutoPtr<world::Map::Impl>::~PrivateAutoPtr() + 21 (libcore.h:387)
32 0x000000010e57290e world::Map::~~Map() + 62 (map.h:77)
33 0x000000010e561bd5 world::Map::~~Map() + 21 (map.h:77)
34 0x000000010e561bf9 world::Map::~~Map() + 25 (map.h:77)
35 0x000000010e4fe9e6 ClientServerWorld::Impl::changeMap(res::MapManifest*) + 198 (clientserverworld.cpp:730)
```

Associated revisions

Revision 440deca9 - 2016-07-25 14:10 - danij

Fixed|World: SIGSEGV during ~Subsector (e.g., icarus.wad MAP01)

IssueID #2167

History

#1 - 2016-07-24 23:07 - danij

- Assignee changed from Deng Team to danij

- % Done changed from 0 to 10

#2 - 2016-07-25 14:13 - danij

- Status changed from New to Closed

- % Done changed from 10 to 100

#3 - 2017-02-25 12:02 - skyjake

- Target version deleted (49)