Doomsday Engine - Bug #2144

Crash when reseting engine with a map loaded

2015-12-25 13:12 - skyjake

Status:	Closed	**Start date:**	2015-12-25
Priority:	Urgent	**% Done:**	100%
Assignee:	Deng Team		
Category:	Defect		
Target version:	2.0 – Home UI & Packages		

Description

Version 1.15.6

- Game: doom1-ultimate
- No additional resources loaded

Start up a game to E1M1, type "reset" in console:

```
Crashed Thread:        0  Dispatch queue: com.apple.main-thread

Exception Type:        EXC_BAD_ACCESS (SIGSEGV)
Exception Codes:       EXC_I386_GPFLT
Exception Note:        EXC_CORPSE_NOTIFY

Thread 0 Crashed:: Dispatch queue: com.apple.main-thread
0   libdeng_core.2.0.0.dylib          0x000000010785b550 de::Record::operator[](de::String const&)
 const + 16
1   libdeng_core.2.0.0.dylib          0x0000000107861e54 de::RecordAccessor::gets(de::String const
&) const + 20
2   net.dengine.doomsday              0x0000000106d862b5 MapDef::composeUri() const + 69
3   net.dengine.doomsday              0x0000000106fd002e de::Map::mapInfo() const + 46
4   net.dengine.doomsday              0x0000000106d964fe GL_TotalRestore() + 78
5   net.dengine.doomsday              0x0000000106d6310e DD_UpdateEngineState() + 286
6   net.dengine.doomsday              0x0000000106d666f9 CCmdReset + 9
7   libdeng_doomsday.1.15.5.dylib     0x00000001084a97e6 Con_CheckExecBuffer() + 2406
8   libdeng_doomsday.1.15.5.dylib     0x00000001084aa6fb Con_Execute + 43
```

Unstable 2.0 build 1819 (OS X with Address Sanitizer)

```
ERROR: AddressSanitizer: heap-use-after-free on address 0x6070007a4f40 at pc 0x000105fc8e3a bp 0x7
fff5fbf7360 sp 0x7fff5fbf7358
READ of size 8 at 0x6070007a4f40 thread T0
    #0 0x105fc8e39 in de::RecordAccessor::accessedRecord() const recordaccessor.cpp:33
    #1 0x105fc8f88 in de::RecordAccessor::get(de::String const&) const recordaccessor.cpp:49
    #2 0x105fc943a in de::RecordAccessor::gets(de::String const&) const recordaccessor.cpp:109
    #3 0x100207809 in res::MapManifest::composeUri() const mapmanifest.h:54
    #4 0x100c60d68 in de::Map::mapInfo() const map.cpp:1546
    #5 0x100221338 in GL_TotalRestore() gl_main.cpp:638
    #6 0x10016cd27 in DD_UpdateEngineState() dd_main.cpp:2253
```

"heap-use-after-free" would suggest that some deleted object is being accessed after the reset.

Associated revisions

Revision b67126be - 2015-12-25 13:30 - skyjake

Fixed|libdoomsday: Avoid a crash when reseting engine state

Map observes when its manifest is deleted.

IssueID #2144

History

#1 - 2015-12-25 13:13 - skyjake

- Description updated

#2 - 2015-12-25 13:13 - skyjake

- Tags set to Resources

#3 - 2015-12-25 13:32 - skyjake

With b67126be1 applied, the problem now is:

```
==73021==ERROR: AddressSanitizer: heap-use-after-free on address 0x606002c277e0 at pc 0x0001007f39f4 bp 0x7fff
5fbf6780 sp 0x7fff5fbf6778
READ of size 4 at 0x606002c277e0 thread T0
    #0 0x1007f39f3 in TextureVariantSpec::operator==(TextureVariantSpec const&) const texturevariant.cpp:149
    #1 0x1007ccc68 in de::Texture::chooseVariant(de::Texture::ChooseVariantMethod, TextureVariantSpec const&,
bool) texture.cpp:193
    #2 0x1007ccdef in de::Texture::chooseVariant(de::Texture::ChooseVariantMethod, TextureVariantSpec const&,
bool) texture.cpp:210
    #3 0x1007cd075 in de::Texture::prepareVariant(TextureVariantSpec const&) texture.cpp:222
    #4 0x1005ca4e1 in R_GetPatchInfo api_resource.cpp:339
    #5 0x1003ac463 in loadViewBorderPatches() r_draw.cpp:74
    #6 0x1003ac136 in R_SetBorderGfx r_draw.cpp:114
    #7 0x112fbb3c0 in R_InitRefresh g_game.cpp:693
    #8 0x112fd87a8 in G_UpdateState g_update.cpp:110
    #9 0x10016cef2 in DD_UpdateEngineState() dd_main.cpp:2282
```

Looks like another case of trying to access objects destroyed during the reset.

#4 - 2016-09-02 13:19 - skyjake

- Status changed from New to Resolved

- Target version set to 2.0 – Home UI & Packages

- % Done changed from 0 to 100

I believe this was fixed when the new package loading UI was implemented, when working on the dialog for automatically loading packages required by a savegame.

#5 - 2016-10-03 09:51 - skyjake

- Status changed from Resolved to Closed