Doomsday Engine - Bug #636

invalid read of 8 byte

2009-03-02 21:55 - gerddie

Status:	Closed	**Start date:**	2009-03-02
Priority:	Normal	**% Done:**	100%
Assignee:	danij		
Category:			
Target version:	1.9.0-beta6		

Description

In Stack_Pop the program tries to read in non-allocated space (see valgrind output below) - apparently, because the stack pointer is first decremented, and then it is read before that pointer.

Attached patch fixes the problem

```
Invalid read of size 8
13714    at 0x4988A3: Stack_Pop (m_stack.c:125)
13714    by 0x4A50E1: R_InitFlats (r_data.c:1510)
13714    by 0x4830A4: DD_StartupWorker (dd_main.c:593)
13714    by 0x4E39B36: SDL_RunThread (SDL_thread.c:202)
13714    by 0x4E706C8: RunThread (SDL_systhread.c:47)
13714    by 0x5094026: start_thread (pthread_create.c:297)
13714    by 0x7245CBC: clone (in /lib64/libc-2.8.so)
13714  Address 0xc9cc1e8 is 8 bytes before a block of size 16 alloc'd
13714    at 0x4C24E21: realloc (vg_replace_malloc.c:429)
13714    by 0x4988DE: Stack_Push (m_stack.c:102)
13714    by 0x4A4EB9: R_InitFlats (r_data.c:1503)
13714    by 0x4830A4: DD_StartupWorker (dd_main.c:593)
13714    by 0x4E39B36: SDL_RunThread (SDL_thread.c:202)
13714    by 0x4E706C8: RunThread (SDL_systhread.c:47)
13714    by 0x5094026: start_thread (pthread_create.c:297)
13714    by 0x7245CBC: clone (in /lib64/libc-2.8.so)
```

PS: Shouldn't the "if (!s)" respective now "if (s)" be an "assert(s)"?

Labels: Data

History

#1 - 2009-03-02 21:55 - gerddie

patch to fix false read

Attachments:

- http://sourceforge.net/p/deng/bugs/_discuss/thread/6f9dca29/aa63/attachment/invalid-read-Stack_Pop-fix.patch

#2 - 2009-03-02 22:52 - danij

Fixed in rev #6434. Well spotted, cheers.