Doomsday Engine - Bug #1000

[Heretic MP] SEGV during item use (2 clients)

2012-03-05 00:21 - bsdtrhodes

Status:	Closed	Start date:	2012-03-05
Priority:	High	% Done:	100%
Assignee:	skyjake		
Category:			
Target version:	1.9.7		
Description			
When playing a network Heretic game, from a dedicated server and two players, using an item causes a SIGSEGV on my CentOS 6.X box. I verified that this happens to both players, items tested were the time bomb, tome of power, and flask. This is the strace output I received:			
read(5, 0x2a982a4, 4096) = 1 EAGAIN (Resource temporarily una			
$\frac{\text{variable}}{\text{ioctl}(6, 0\text{xc}0284658, 0\text{x}7ffff25b8bc0}) = 0$			
1000000000000000000000000000000000000			
$\frac{\text{ioctl}(6, 0 \times 0.0284658, 0 \times 7ffff25b8bc0)}{\text{ioctl}(6, 0 \times 0.0284658, 0 \times 7ffff25b8bc0)} = 0$			
ioctl(6, 0xc0284658, 0x7ffff25b8bc0) = 0			
ioctl(6, 0xc0104629, 0x7ffff25b8bb0) = 0			
$\frac{close(5)}{close(5)} = 0$			
poll([[fd=4, events=POLLIN POLLOUT]], 1, -1) = 1 ([[fd=4, revents=POLLOUT]])			
writev(4, [{"<\2\2\0\0\0\3+\0\1\0", 12}, {NULL, 0}, {"", 0}], 3) = 12			
poll([[fd=4, events=POLLIN]], 1, -1) = 1 ([[fd=4, revents=POLLIN]])			
read(4, "\1\1\264\0\0\0\0\0\32\0\240\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0			
0", 4096) = 32			
read(4, 0x2a882e4, 4096) = -1 EAGAIN (Resource temporarily una			
vailable)			
close(4) = 0			
munmap(0x3e5ee00000, 2128136) = 0			
rt_sigaction(SIGSEGV, NULL, {SIG_DFL, [SEGV], SA_RESTORER SA_RESTART, 0x3e556			
32900}, 8) = 0			
rt_sigaction(SIGBUS, NULL, {0x3e74008990, [], SA_RESTORER, 0x3e5620f4a0}, 8)			
rt_sigaction(SIGBUS, {SIG_DFL, [], SA_RESTORER, 0x3e5620f4a0}, NULL, 8) = 0			

rt_sigaction(SIGFPE, {SIG_DFL, [], SA_RESTORER, 0x3e5620f4a0}, NULL, 8) = 0 rt_sigaction(SIGQUIT, NULL, {0x3e74008990, [], SA_RESTORER, 0x3e5620f4a0}, 8)

rt_sigaction(SIGFPE, NULL, {0x3e74008990, [], SA_RESTORER, 0x3e5620f4a0}, 8)

rt_sigaction(SIGQUIT, {SIG_DFL, [], SA_RESTORER, 0x3e5620f4a0}, NULL, 8) = 0

tgkill(4757, 4757, SIGSEGV) - 0

rt_sigreturn(0x1295) = 139856630083200

SIGSEGV (Segmentation fault) @ 0 (0) ---

++ killed by SIGSEGV ++

Segmentation fault

Let me know if you want a core dump, I can enable cores and try to produce one.

Labels: jHeretic

History

#1 - 2012-03-04 22:56 - skyjake

Fixed for 1.9.8 (in Friday's build #476).

The client was attempting to play the Use sound of an invalid inventory item.

2024-04-09 1/1