Doomsday Engine - Bug #1954

Joining an MP game from a different game causes segfault (after version conflict)

2015-01-29 00:34 - vermil

Status:	Closed	**Start date:**	2015-01-29
Priority:	Urgent	**% Done:**	100%
Assignee:	skyjake		
Category:	Defect		
Target version:	1.15		

Description

Attempting to join an MP game from a different game causes a seg fault in the latest unstable (1486). For instance attempting to join a Doom2 MP game while running Ultimate Doom.

Attempting to join an MP game from the same game one is currently running appears to function correctly.

This seems to be a bug that has been around a fair while.

Related issues:

Related to Bug #1960: Crash when handling input events during busy mode	**Closed**	**2015-02-05**

Associated revisions

Revision d93e3fe3 - 2015-02-09 11:00 - skyjake

Fixed|UI|Multiplayer: Potential crash when joining an MP game

Synchronous signal handling (game unload, MP join) may lead to the widget being gone when it's time to check if there's a further action to do.

IssueID #1954

Revision 3e1527da - 2015-02-11 19:22 - skyjake

Fixed|Multiplayer|Client: Cleaning up client state when leaving a game

The client was not properly cleaning its state when leaving a game. Now received packets are discarded and the postfx shader is reset to "none".

If one was kicked from an MP game due to version conflict, the old buffered packets caused a segfault when the client continued handling them after connecting to a new server.

IssueID #1954
IssueID #1971

History

#1 - 2015-01-29 02:11 - danij

- Category set to Defect

- Priority changed from Normal to Urgent

- Target version set to 49

#2 - 2015-01-30 21:52 - skyjake

- Status changed from New to In Progress

- Assignee set to skyjake

#3 - 2015-01-31 14:10 - skyjake

I tried this on OS X with two local servers, but it didn't trigger any problems. Next I'll have to set up suitable remote servers and try it on Windows.

BTW, were you using any resource packs in these games?

#4 - 2015-02-01 15:52 - skyjake

Tried local servers on Windows (without resource packs), didn't get a crash.

#5 - 2015-02-02 11:17 - vermil

I wasn't using any resource packs and was trying to join a non-local server.

Specifically, various ones of Kuri Kai.

It could be a version mis-match (and that causes a seg fault when one tries to join a server with a different version from a game other than the one the MP game is for).

#6 - 2015-02-05 15:59 - skyjake

- Related to Bug #1960: Crash when handling input events during busy mode added

#7 - 2015-02-05 15:59 - skyjake

- Subject changed from Joining an MP game from a different game to Joining an MP game from a different game causes segfault

#8 - 2015-02-05 16:16 - skyjake

During my Windows debugging I discovered and fixed #1960, which may have been the primary culprit here, since it was possible to trigger it also with key/mouse release events.

Needs to be tested again with Friday's build (or later). I'll keep the MP test servers running for convenience (occasionally if not all the time).

#9 - 2015-02-05 16:24 - skyjake

- Status changed from In Progress to Feedback

- Assignee changed from skyjake to vermil

- % Done changed from 0 to 20

#10 - 2015-02-09 06:46 - eunbolt

- File gdb_output_build1500_20150209.txt added

Attached is the gdb output of the crash on my system using build 1500.

not a debug build

#11 - 2015-02-09 06:49 - eunbolt

the above gdb output is the server and the client on the local machine, so both are build 1500.(not the nz/au servers)

vermil's test from above are most likely to the nz/au. whcich he is correct that they are version mismatches as they are the latest stable build

#12 - 2015-02-09 06:54 - skyjake

That does show a crash occurring, however without debug symbols it doesn't help much. Any chance you could do a debug build? That would be extremely helpful.

I'll try local servers on Linux myself and see if I can reproduce it.

#13 - 2015-02-09 07:53 - eunbolt

- File gdb_output_build1500_20150209.2.txt added

attached is from a 1500build that had debug as an option

config_user.pri contained

```
CONFIG += deng_extassimp
CONFIG += deng_debug
PREFIX=/opt/deng1500
```

#14 - 2015-02-09 08:01 - eunbolt

attached now is the output from a debug build

config_user.pri contained

CONFIG += deng_extassimp
CONFIG += deng_debug
PREFIX=/opt/deng1500

#15 - 2015-02-09 08:51 - skyjake

From the .2 log:

> Reading symbols from doomsday...(no debugging symbols found)...done.
> Executable: Doomsday Engine 1.15.0 (Unstable 64-bit) Feb 9 2015 18:18:11

Did you rerun qmake after modifying config_user.pri and do a clean rebuild? This should say "Unstable 64-bit +D +R", and gdb should be finding debug symbols.

> CONFIG+=deng_debug

This should be just "CONFIG+=debug".

#16 - 2015-02-09 09:59 - eunbolt

- File gdb_output_build1500_20150209.3.txt added

ok, here is debug build output

#17 - 2015-02-09 10:00 - eunbolt

debug build output uploaded

#18 - 2015-02-09 10:01 - skyjake

Thanks! That indicates the crash is caused by the UI widget, I'll look into it.

#19 - 2015-02-09 11:01 - skyjake

- Status changed from Feedback to In Progress

- Assignee changed from vermil to skyjake

- % Done changed from 20 to 40

#20 - 2015-02-11 15:26 - skyjake

I've fixed the likely cause of the crash in the UI widget. A new build will be available later today for testing.

#21 - 2015-02-11 19:22 - skyjake

- % Done changed from 40 to 80

#22 - 2015-02-11 19:24 - skyjake

I discovered and fixed another crash. Just as vermil suggested, first having a version conflict with a server and then joining another was causing invalid network packets to be buffered on the client. I've now fixed this for the next build (not in 1502).

#23 - 2015-02-11 19:49 - skyjake

- Subject changed from Joining an MP game from a different game causes segfault to Joining an MP game from a different game causes segfault (after version conflict)

#24 - 2015-02-17 12:37 - skyjake

- Target version changed from 49 to 1.15

#25 - 2015-02-24 19:01 - skyjake

- Status changed from In Progress to Closed

- % Done changed from 80 to 100

Files

gdb_output_build1500_20150209.txt	17.7 KB	2015-02-09	eunbolt
gdb_output_build1500_20150209.2.txt	17.9 KB	2015-02-09	eunbolt
gdb_output_build1500_20150209.3.txt	25.4 KB	2015-02-09	eunbolt