Doomsday Engine - Bug #2019

ST_UILogForPlayer returning garbage in jDoom64

2015-04-30 07:32 - rhargrave

Status:	Closed	**Start date:**	2015-04-30
Priority:	Normal	**% Done:**	100%
Assignee:	rhargrave		
Category:	Defect		
Target version:			

Description

This appears to be the current *major* crash issue in jD64.

I've been debugging it on the CMake branch using GDB, and the engine reliably crashes due to a failed assertion in the memory manager (specifically, Z_Realloc). What it looks like is going on becomes apparent in UILog_Push. Essentially, what I'm seeing is that UILog_Post/Push are being passed garbage in place of the parameter `ob`, UILog_Push then goes to get the index of the next available chat message, which is more than likely out of bound. In the event that it has to lengthen the string for that line, it will call `Z_Realloc`. Said string, having never been allocated in the first place, will simply cause `Z_Realloc` to raise an exception (as the object is not inside managed space) which goes uncaught.

Related issues:

Related to Feature #1580: Fix the Doom 64: Absolution TC plugin	**New**	**2015-04-30**
Related to Bug #2025: Doom64TC does not have a fully functional HUD	**Progressed**	**2015-05-02**

History

#1 - 2015-04-30 08:06 - skyjake

- Related to Feature #1580: Fix the Doom 64: Absolution TC plugin added

#2 - 2015-05-02 22:49 - rhargrave

I've been debugging this, and this is what's going on:

- `UILog_Push` wants to reallocate a log message using `Z_Realloc`
- This message's memory is either not managed, or was allocated using `M_Malloc(size_t)`, or `malloc(size_t)` and does not reside in contiguous space managed by `memoryzone`.
- `Z_Realloc` aborts due to the above

#3 - 2015-05-03 00:30 - rhargrave

- Related to Bug #2025: Doom64TC does not have a fully functional HUD added

#4 - 2015-05-03 00:30 - rhargrave

- Status changed from New to Closed

- Assignee set to rhargrave

- % Done changed from 0 to 100

Fixed by #2025

#5 - 2015-05-03 07:24 - skyjake

- Tags changed from Doom64 to Doom64TC