Kerbal Space Program - Bug #752

KSP crashes on startup

06/02/2013 02:03 PM - Vorpal

Status:	Closed	**Start date:**	06/02/2013
Severity:	Low	**% Done:**	100%
Assignee:			
Category:	Gameplay		
Target version:			
Version:	0.20.2	**Language:**	English (US)
Platform:	Linux	**Mod Related:**	No
Expansion:			

Description

What happens
On my Linux system both KSP.x86 and KSP.x86_64 crashes on startup. The GUI shows up and begin loading resources. Once it gets to "Squad/Flags/09" in the progress bar text it crashes with "Aborted (core dumped)". This happens on every attempt.

Notes

- This happened on 0.19.1 (the first version I tried, since I bought the game at that point) and the current 0.20.2.
- I have a core dump if you want me to send it to you. It is however 368 MB (76 MB when compressed with xz), so I don't know how I would do that... Dropbox? Tell me if you want this and I'll try to find a way.
- KSP.log and Player.log are attached.

System info

- Core i5 (Sandy Bridge) @ 3.3 GHz
- 16 GB RAM
- AMD Radeon HD 6850 GPU (using propritary drivers, Debian package manager (aptitude) says version of fglrx-driver is 1:12-6+point-3)
- uname -a: Linux tux 3.2.0-4-amd64 #1 SMP Debian 3.2.41-2+deb7u2 x86_64 GNU/Linux
- Debian Wheezy (7.0) x86_64.

History

#1 - 06/02/2013 02:03 PM - Vorpal

Sorry for the screwed up formatting, I have no idea how that happened...

#2 - 06/02/2013 09:36 PM - a.g.

- File Player.log added

I had a crash at the same address as the above log, and when I tried looking at the instruction where it crashed, I found some obviously 32-bit code in the supposedly 64-bit process:

=> 0x0000000000bcec9f: mov   al,BYTE PTR [edi+ebx*1]

After some searching it turned out that this code came from optimized inline assembly in this file of libpng 1.2.18, which obviously should never be enabled in a 64-bit build: http://svn.ghostscript.com/ghostscript/tags/libpng-1.2.18/pngvcrd.c (comparison http://pastebin.com/599g7h7i). Interestingly, this file with all the assembly code is removed in libpng 1.2.20.

This means that until fixed/patched the 64-bit build will crash whenever it loads a png image that uses one of the optimized code paths, and the relevant buffers are not within the low 2 GB of the address space (which depends on kernel & library settings, and chance).

Edit: even a better match of the disassembly is the same function from http://svn.ghostscript.com/ghostscript/tags/libpng-1.2.18/pnggccrd.c (sort of obvious in hindsight, since it is for gcc, while the other is for msvc).

#3 - 06/03/2013 06:29 PM - Ted

- Description updated

- Severity changed from Critical to High

Corrected some formatting and lowered the priority a bit.
Don't worry about the formatting though. :)

#4 - 06/04/2013 10:42 AM - Vorpal

a.g. wrote:

> This means that until fixed/patched the 64-bit build will crash whenever it loads a png image that uses one of the optimized code paths, and the relevant buffers are not within the low 2 GB of the address space (which depends on kernel & library settings, and chance).

This does not explain why the 32-bit version also crashes like that though.

#5 - 06/04/2013 01:40 PM - a.g.

You didn't post the Player.log for the 32-bit version - it actually contains some useful stack traces.

Btw, for the last 2 days I've been running with KSP.x86_64 where I changed bytes 7cebc7 and 7cebcc from 01 to 00 so as to make png_mmx_support from that pnggccrd.c always return 0, and that seems to have solved the crash I was having.

#6 - 06/04/2013 01:44 PM - Vorpal

- File Player.log added

It does indeed seem that the 32-bit crash is different from the 64-bit crash, it happens much earlier for a start.

I attached a 32-bit Player.log as well

#7 - 06/04/2013 01:52 PM - Vorpal

- File Player.log added

- File KSP.log added

I applied your suggestion to the 64-bit binary and it did get much further before crashing (Kerbals on the loading screen background, last observed text was "Squad/Parts/Engine/engineLargeSkipper/model001"). Here is a new Player.log.

#8 - 06/04/2013 02:47 PM - a.g.

Now it seems both crash in the fglrx stuff - can't help there unfortunately.

#9 - 06/06/2013 06:03 PM - Anonymous

- Severity changed from High to Unworthy

Changed the priority to unworthy because KSP does not support Debian. There is a good thread in the Support forum where many linux user may be able to help you though :)

http://forum.kerbalspaceprogram.com/showthread.php/24529-The-Linux-compatibility-thread!

#10 - 06/14/2013 02:37 PM - th3flyboy

This problem is also happening in Linux Mint 15 which is using the Ubuntu Raring repos for the libraries in question. Thus the problem is also appearing on Ubuntu and Ubuntu spinoffs.

Just because the distro isn't supported doesn't mean this isn't worthy if the problem can be traced back to a dependency as was traced here. This is a problem caused by the library, not the distro.

If need be I can pop Ubuntu Raring on a virtual machine just to prove that this isn't a distro specific problem.

#11 - 08/16/2013 10:39 AM - Ted

- Category set to Gameplay

- Severity changed from Unworthy to Low

Could you check to see whether this issue is still present in 0.21.1?

#12 - 08/17/2013 04:09 PM - Vorpal

I tried it, and I get the same crashes. The 32-bit version crashes just as early as before. The 64-bit version also crashes like before. Since I do not know the proper offset for the png fix for the 64-bit edition of the new version, I can not properly test that partial workaround. I'm not super-keen on trying to reverse engineer x86 assembly.

Worth noting is that my computer setup changed since I originally filed the bug, I now run a dual monitor setup (24" 1920x1200 + 22" 1680x1050). Other than that, it is the same.

#13 - 08/17/2013 04:27 PM - Ted

Does it occur without the flgrx drivers?

#14 - 08/26/2013 10:45 AM - Vorpal

Yes, in all cases I'm using fglrx. (Sorry for the slow response, I have been on a trip without internet for the past 8 days.) Driver version is still 1:12-6+point-3 according to the package manager.

#15 - 10/25/2013 06:21 PM - sr

The way I read his report, it's an issue with debian-derivitives distributing a library which has been incorrectly compiled. I'm not sure if Squad can do anything here, it's an upstream issue.

I've just checked both the debian and ubuntu bugtrackers for libpng-12, and both don't seem have any open issues that correlate with a.g.s deductions. I'd recommend pursuing this issue with the distros, as KSP cannot be the only one affected by such an issue.

(unless of course I'm reading this wrong, and the culprit isn't a libpng.so, but a .a library that got statically compiled into unity, in which case unity should get petitioned to clean up its compilation environment).

#16 - 11/04/2013 02:28 PM - a.g.

Well, since the patch is for the main ksp executable, it follows that it is indeed a statically linked library in unity. ;)

It would be interesting to see if this is fixed in the next release, which apparently would use a new unity version, unlike all the releases from 0.20.2 to 0.22.

#17 - 12/06/2013 08:09 AM - stock

- Status changed from New to Confirmed

- % Done changed from 0 to 10

I wanted to confirm that this bug continues to exist in 0.22 and that the binary patch to the KSP.x86_64 binary fixes it. I'm running on a box that has 24GB of memory and with the fix KSP has been working great.

As an aside a.g., this is a seriously hardcore bugfix. I haven't had to patch a binary like this since I was cracking games in the 80's. Awesome.
-Matt

#18 - 11/20/2015 12:47 PM - sal_vager

- Status changed from Confirmed to Need More Info

- % Done changed from 10 to 0

Can some one please retest this issue on a current KSP build and current Debian drivers, it'd be nice to know if it's fixed.

#19 - 07/17/2016 09:40 AM - TriggerAu

- Status changed from Need More Info to Needs Clarification

#20 - 08/07/2016 11:33 AM - TriggerAu

- Status changed from Needs Clarification to Closed

- % Done changed from 0 to 100

Closing this report out for now. If you find it is still occuring in the latest version of KSP please open a new report (and this one can be linked to it.) For best results, the wiki contains really useful info for when creating a report http://bugs.kerbalspaceprogram.com/projects/ksp/wiki.

You can also ask questions about the bug cleanup in the forum here:
http://forum.kerbalspaceprogram.com/index.php?/topic/143980-time-to-clean-up-the-bug-tracker/ and tag @TriggerAu to get my attention

Files

KSP.log	1.84 KB	06/02/2013	Vorpal
Player.log	14.3 KB	06/02/2013	Vorpal
Player.log	401 KB	06/02/2013	a.g.
Player.log	9.41 KB	06/04/2013	Vorpal
Player.log	35.3 KB	06/04/2013	Vorpal