

# Kerbal Space Program - Bug #5530

## Reproducible Segmentation fault when quitting.

10/10/2015 01:04 PM - lebedev.ri

<b>Status:</b> Closed	<b>Start date:</b> 10/10/2015
<b>Severity:</b> Low	<b>% Done:</b> 100%
<b>Assignee:</b>	
<b>Category:</b> Application	
<b>Target version:</b>	
<b>Version:</b> 1.0.4	<b>Language:</b> English (US)
<b>Platform:</b> Any	<b>Mod Related:</b> No
<b>Expansion:</b>	

### Description

Debian sid, fglrx.

No mods, absolutely new, clean install, even no changed settings.

Happens even if i just start KSP, and then immediately quit.

Once i quit, the last entry in terminal is:

```
$. /KSP.x86_64
Set current directory to ~/KSP_linux/KSP_linux
Found path: ~/KSP_linux/KSP_linux/KSP.x86_64
Mono path[0] = '~/KSP_linux/KSP_linux/KSP_Data/Managed'
Mono path[1] = '~/KSP_linux/KSP_linux/KSP_Data/Mono'
Mono config path = '~/KSP_linux/KSP_linux/KSP_Data/Mono/etc'
/dev/input/js0: driver version: 2.1.0 (20100)
: Too many axes; using axes 0 - 19 and ignoring axes 20 - 36
: Too many buttons; using buttons 0 - 19 and ignoring buttons 20 - 68
/dev/input/js0: fd 3, buttons 20, axes 20, name A4TECH USB Device
/dev/input/js0: axis 0: raw -32767, mapped 0.000000
/dev/input/js0: axis 1: raw -32767, mapped 0.000000
/dev/input/js0: axis 2: raw -32767, mapped 0.000000
/dev/input/js0: axis 3: raw -32767, mapped 0.000000
/dev/input/js0: axis 4: raw -32767, mapped 0.000000
/dev/input/js0: axis 5: raw -32767, mapped 0.000000
/dev/input/js0: axis 6: raw -32767, mapped 0.000000
/dev/input/js0: axis 7: raw -32767, mapped 0.000000
/dev/input/js0: axis 8: raw -32767, mapped 0.000000
/dev/input/js0: axis 9: raw -32767, mapped 0.000000
/dev/input/js0: axis 10: raw 0, mapped 0.000000
/dev/input/js0: axis 11: raw 0, mapped 0.000000
/dev/input/js0: axis 12: raw -32767, mapped 0.000000
/dev/input/js0: axis 13: raw -32767, mapped 0.000000
/dev/input/js0: axis 14: raw -32767, mapped 0.000000
/dev/input/js0: axis 15: raw -32767, mapped 0.000000
/dev/input/js0: axis 16: raw -32767, mapped 0.000000
/dev/input/js0: axis 17: raw -32767, mapped 0.000000
/dev/input/js0: axis 18: raw -32767, mapped 0.000000
/dev/input/js0: axis 19: raw -32767, mapped 0.000000
/dev/input/js0: axis 20: raw -32767, mapped 0.000000
Segmentation fault
```

This happens every time.

### History

#1 - 10/10/2015 01:15 PM - lebedev.ri

And in dmesg:

```
[13655.912293] traps: KSP.x86_64[16658] general protection ip:7ff1573bf377 sp:7fff81a50940 error:0 in libX11.so.6.3.0[7ff157399000+13c000]
[23603.890178] traps: KSP.x86_64[10660] general protection ip:7f6b8555f377 sp:7ffca7374620 error:0 in libX11.so.6.3.0[7f6b85539000+13c000]
```

**#2 - 10/10/2015 01:20 PM - lebedev.ri**

**gdb:**

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff702a377 in XForceScreenSaver (dpy=0x1a42da0, mode=1) at ../../src/FSSaver.c:53
53      ../../src/FSSaver.c: No such file or directory.
(gdb) thread apply all bt full
```

```
Thread 2 (Thread 0x7ffff7fdc700 (LWP 12470)):
#0  0x00007ffff79ca18d in nanosleep () at ../sysdeps/unix/syscall-template.S:81
No locals.
#1  0x00007ffff4fd214d in ?? () from /home/lebedevri/KSP_linux/KSP_linux/KSP_Data/Mono/x86_64/libmono.so
No symbol table info available.
#2  0x00007ffff79c30a4 in start_thread (arg=0x7ffff7fdc700) at pthread_create.c:309
    __res = <optimized out>
    pd = 0x7ffff7fdc700
    now = <optimized out>
    unwind_buf = {cancel_jmp_buf = {{jmp_buf = {140737353991936, 1365188317788037865, 0, 140737354125408,
140737302984492, 140737353991936, -1365170740629544215, -1365170461010369815}, mask_was_saved = 0}}, priv = {p
ad = {0x0, 0x0, 0x0, 0x0}, data = {prev = 0x0,
    cleanup = 0x0, canceltype = 0}}}
    not_first_call = <optimized out>
    pagesize_ml = <optimized out>
    sp = <optimized out>
    freesize = <optimized out>
    __PRETTY_FUNCTION__ = "start_thread"
#3  0x00007ffff62a406d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111
No locals.
```

```
Thread 1 (Thread 0x7ffff7fb4740 (LWP 12466)):
#0  0x00007ffff702a377 in XForceScreenSaver (dpy=0x1a42da0, mode=1) at ../../src/FSSaver.c:53
    req = <optimized out>
#1  0x000000000042dffd in ?? ()
No symbol table info available.
#2  0x00007ffff61dfb45 in __libc_start_main (main=0x42d0c0, argc=1, argv=0x7fffffffdeb8, init=<optimized out>,
fini=<optimized out>, rtd_fini=<optimized out>, stack_end=0x7fffffffdea8) at libc-start.c:287
    result = <optimized out>
    unwind_buf = {cancel_jmp_buf = {{jmp_buf = {0, 1365188317788037865, 4388968, 140737488346800, 0, 0, -1
365188318798224663, -1365167169268161815}, mask_was_saved = 0}}, priv = {pad = {0x0, 0x0, 0x1290df0, 0x7fffffff
fdeb8}, data = {prev = 0x0, cleanup = 0x0,
    canceltype = 19467760}}}
    not_first_call = <optimized out>
#3  0x000000000042f891 in ?? ()
No symbol table info available.
#4  0x00007fffffffdea8 in ?? ()
No symbol table info available.
#5  0x000000000000001c in ?? ()
No symbol table info available.
#6  0x0000000000000001 in ?? ()
No symbol table info available.
#7  0x00007ffffffe223 in ?? ()
No symbol table info available.
#8  0x0000000000000000 in ?? ()
No symbol table info available.
```

**#3 - 07/17/2016 09:39 AM - TriggerAu**

- Status changed from New to Needs Clarification

**#4 - 08/09/2016 01:47 PM - lebedev.ri**

- Status changed from Needs Clarification to Resolved

- % Done changed from 0 to 100

**#5 - 10/13/2016 11:16 AM - TriggerAu**

- Status changed from Resolved to Closed