# DragonFlyBSD - Bug #1975

## Applications seg fault in select() and poll()

01/28/2011 11:56 PM - rumcic

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |

**Description**

On recent -master I have noticed that I can make knode (from kde3) crash (bus error) in select() repeatably and have even managed to crash firefox once. All crashes seem to be identical.

knode:
Program terminated with signal 10, Bus error.
#0 0x29f7a03b in select () at select.S:2
2 RSYSCALL(select)
(gdb) bt
#0 0x29f7a03b in select () at select.S:2
#1 0x29cf1d8b in __select (numfds=1024, readfds=0xbf9feee0, writefds=0x0, exceptfds=0xbf9fee60, timeout=0xbf9fef60)
at /usr/src/lib/libthread_xu/thread/thr_syscalls.c:518
#2 0x293430d3 in KSocks::select (this=0x2a9474c8, n=1024, readfds=0xbf9feee0, writefds=0x0, exceptfds=0xbf9fee60, timeout=0x4) at ksocks.cpp:576
#3 0x2812b280 in KNProtocolClient::waitForWork() ()
from /usr/pkg/lib/libknodecommon.so.3
#4 0x2812b499 in KNProtocolClient::run() ()
from /usr/pkg/lib/libknodecommon.so.3
#5 0x29688679 in QThreadInstance::start (_arg=0x2aa63fa4) at kernel/qthread_unix.cpp:119
#6 0x29cf3eb7 in thread_start (arg=0x2a020cb0)
at /usr/src/lib/libthread_xu/thread/thr_create.c:242
#7 0x00000000 in ?? ()

firefox:
(gdb) bt
#0 0x2a67691b in poll () at poll.S:2
#1 0x28094fc2 in __poll (fds=0xbf9feb24, nfds=1, timeout=-1)
at /usr/src/lib/libthread_xu/thread/thr_syscalls.c:407
#2 0x29b4ac7c in _pr_poll_with_poll (pds=0x2aed0c68, npds=1, timeout=4294967295) at ptio.c:3915
#3 PR_Poll (pds=0x2aed0c68, npds=1, timeout=4294967295) at ptio.c:4317
#4 0x28555b01 in nsSocketTransportService::Poll (this=0x2aed0780, wait=1, interval=0xbf9fedb4) at nsSocketTransportService2.cpp:355
#5 0x285568c4 in nsSocketTransportService::DoPollIteration (this=0x2aed0780, wait=1) at nsSocketTransportService2.cpp:660
#6 0x28556c0b in nsSocketTransportService::OnProcessNextEvent (this=0x2aed0780, thread=0x2ac12500, mayWait=1, depth=1)
at nsSocketTransportService2.cpp:539
#7 0x296ac231 in nsThread::ProcessNextEvent (this=0x2ac12500, mayWait=1, result=0xbf9fee6c) at nsThread.cpp:508
#8 0x29647714 in NS_ProcessNextEvent_P (thread=0x0, mayWait=1) at nsThreadUtils.cpp:250
#9 0x285573b1 in nsSocketTransportService::Run (this=0x2aed0780) at nsSocketTransportService2.cpp:581
#10 0x296ac33f in nsThread::ProcessNextEvent (this=0x2ac12500, mayWait=1, result=0xbf9fef2c) at nsThread.cpp:527
#11 0x29647714 in NS_ProcessNextEvent_P (thread=0x0, mayWait=1) at nsThreadUtils.cpp:250
#12 0x296ad7dd in nsThread::ThreadFunc (arg=0x2ac12500) at nsThread.cpp:254
#13 0x29b50122 in _pt_root (arg=0x2ac504d0) at ptthread.c:228

#14 0x28096eb7 in thread_start (arg=0x2ab90690)
at /usr/src/lib/libthread_xu/thread/thr_create.c:242
#15 0x00000000 in ?? ()
--
Please do not CC me, since I already receive everything from these MLs.

Regards,
Rumko

### History

#### #1 - 02/13/2011 06:53 AM - pavalos

On Sat, Jan 29, 2011 at 12:53:54AM +0100, Rumko wrote:
> On recent -master I have noticed that I can make knode (from kde3) crash (bus
> error) in select() repeatably and have even managed to crash firefox once. All
> crashes seem to be identical.
>

I'm seeing this on firefox when I try to use a smart card reader.

--Peter