

PiBox - Bug #257

Default surf crashes

09 Jan 2014 20:43 - Hammel

Status:	In Progress	Start date:	09 Jan 2014
Priority:	Low	Due date:	
Assignee:	Hammel	% Done:	50%
Category:	04 - Root File System	Estimated time:	0.00 hour
Target version:	3.0 - Corrino		
Severity:	05 - Very Low		
Description			
Rev to master in git tree. I've got the update to surf.mk in the build tree and a patch to fix a problem with a DOM update applied since 0.6 to the git tree.			

Associated revisions

Revision c8f8f88c - 10 Jan 2014 21:10 - Hammel

RM #257: Bump surf to git master and fix bug in master related to some DOM incompatibility with webkit.

History

#1 - 10 Jan 2014 21:11 - Hammel

- % Done changed from 0 to 50

Updated applied and build tested. Built version has been copied to target and verified working.

Updates pushed upstream.

Now I just need to make sure it ends up in the release build.

#2 - 14 Jan 2014 20:10 - Hammel

- Status changed from New to Closed

- % Done changed from 50 to 100

Verified working on both Fedora 19 and CentOS 6.4.

Closing issue.

#3 - 27 Feb 2014 20:40 - Hammel

- Status changed from Closed to In Progress

- % Done changed from 100 to 50

Reopening because surf broke with 3.10.x/Buildroot 2013.11. I have no idea what the problem is but suspect its webkitgtk, which also causes midori to crash.

There are no meaningful patches applied to webkitgtk since 2013.11. So although there may be a new Buildroot release (2014.02 is out) I don't think

it will make a difference.

Note: I'm building surf off of master so maybe setting an earlier git id, such as one from mid/late January would be preferable.

#4 - 28 Feb 2014 20:47 - Hammel

- Target version changed from 0.7.0 to 0.8.0

#5 - 01 Mar 2014 21:36 - Hammel

Tried to rev to 1.11.92 from 1.11.5 (which is actually a short jump) but the former requires a gcc 4.7 or later. That means I need to rev Crosstool-NG first. That's a major project. So I can't rev webkit.

This just leaves trying to build surf with webkitgtk 1.11.5 and fixing whatever is causing the crash.

#6 - 02 Mar 2014 14:27 - Hammel

I recompiled surf with debugging symbols enabled (see attached modified surf.mk). I then installed the xcc-debug pkg and ran surf under gdb. This is what I got.

```
(gdb) set args http://localhost:2001
(gdb) run
Starting program: /root/surf http://localhost:2001
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/libthread_db.so.1".
[New Thread 0xb2e37340 (LWP 1955)]
[New Thread 0xb250f340 (LWP 1956)]
[New Thread 0xb1bc6340 (LWP 1957)]
[New Thread 0xb0dd6340 (LWP 1958)]

Program received signal SIGSEGV, Segmentation fault.
0xb3386c60 in JSC::CodeBlock::bytecodeOffset(JSC::ExecState*, JSC::ReturnAddressPtr) ()
    from /usr/lib/libjavascriptcoregtk-1.0.so.0
(gdb) bt
#0  0xb3386c60 in JSC::CodeBlock::bytecodeOffset(JSC::ExecState*, JSC::ReturnAddressPtr) ()
    from /usr/lib/libjavascriptcoregtk-1.0.so.0
#1  0xb34c855c in JSC::jitThrow(JSC::JSGlobalData*, JSC::ExecState*, JSC::JSValue, JSC::ReturnAddressPtr) ()
    from /usr/lib/libjavascriptcoregtk-1.0.so.0
#2  0xb34f3ffc in JITStubThunked_vm_throw () from /usr/lib/libjavascriptcoregtk-1.0.so.0
#3  0xb34e9120 in cti_vm_throw () from /usr/lib/libjavascriptcoregtk-1.0.so.0
#4  0xb34e9120 in cti_vm_throw () from /usr/lib/libjavascriptcoregtk-1.0.so.0
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
```

It looks like its a javascript problem in webkitgtk. So I think the solution may be to rev the toolchain (to get gcc 4.7+ because webkit 2.x requires it) and then try to rev webkit to the stable 2.x version, then rebuild surf against that. See RM #172.

#7 - 08 Mar 2014 16:08 - Hammel

- Priority changed from Immediate to Low

- Target version changed from 0.8.0 to 3.0 - Corrino

- Severity changed from 01 - Critical to 05 - Very Low

I tried webkit 2.0.4 but can't get it to build. I rebuilt with gcc 4.7.3 (non-linaro) and surf behaved slightly better but still crashes. So does midori.

So I'm punting on a native browser for PiBox. There's no point wasting more time on this. I can just enable the settings page for non-local users and then look into an authentication mechanism I can overlay on that.

Moving this to very low priority and will revisit it much later.

#8 - 11 Nov 2014 09:46 - Hammel

Alternative browsers

1. Midori - already part of buildroot - requires webkit
2. [Abaco](#) - no javascript
3. [NetSurf](#) - has its own rendering engine - No javascript