Ports - Bug #8

[libwebkit] segfault in libjavascriptcore-gtk-1.0.so.0

2012-02-18 01:11 PM - mtjm

Status:	fixed	**% Done:**	0%
Priority:	broken		
Assignee:	mtjm		
Category:			

Description

```
mtjm@earendil:~$ gdb midori
GNU gdb (GDB) 7.3.1
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "mips64el-unknown-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
/home/mtjm/.gdbinit:1: Error in sourced command file:
No symbol table is loaded.  Use the "file" command.
Reading symbols from /usr/bin/midori...(no debugging symbols found)...done.
(gdb) r
Starting program: /usr/bin/midori
[Thread debugging using libthread_db enabled]
[New Thread 0x736ab320 (LWP 12391)]
[New Thread 0x72cff320 (LWP 12410)]
[New Thread 0x723ff320 (LWP 12412)]
[New Thread 0x6db53320 (LWP 12623)]

Program received signal SIGSEGV, Segmentation fault.
0x75c56eac in JITStubThunked_op_put_by_id_direct ()
   from /usr/lib/libjavascriptcoregtk-1.0.so.0
(gdb) bt
#0  0x75c56eac in JITStubThunked_op_put_by_id_direct ()
   from /usr/lib/libjavascriptcoregtk-1.0.so.0
#1  0x75c53bb0 in cti_op_put_by_id_direct ()
   from /usr/lib/libjavascriptcoregtk-1.0.so.0
Backtrace stopped: frame did not save the PC
(gdb) q
A debugging session is active.

        Inferior 1 [process 12160] will be killed.

Quit anyway? (y or n) y
```

Surprisingly, rebuilding libjavascriptcoregtk-1.0.so.0 with debug symbols and without optimization and LD_PRELOADing it makes Midori work.

Do we have build logs for the packaged libwebkit? Maybe it enabled JIT, it shouldn't use the functions listed in the backtrace otherwise.

History

#2 - 2012-02-18 05:06 PM - fauno

Michał Masłowski wrote:

> Do we have build logs for the packaged libwebkit? Maybe it enabled JIT, it shouldn't use the functions listed in the backtrace otherwise.

Here they are, I did two passes because the first build failed.

#3 - 2012-02-19 11:53 AM - mtjm

JIT is enabled despite configure saying otherwise. Next build should fix this.

#4 - 2012-02-28 07:54 PM - fauno

randomly browsing with midori and libwebkit-1.6.3-1.1-mips64el doesn't produce crashes :D

#5 - 2012-05-06 01:03 PM - mtjm

Released a new package.

#6 - 2016-05-12 12:23 AM - Anonymous

- Project changed from 3 to Ports

Files

libwebkit-1.6.3-1-mips64el-build.log.1.tar.xz	209 KB	2012-02-18	fauno
libwebkit-1.6.3-1-mips64el-build.log.tar.xz	184 KB	2012-02-18	fauno