

Ruby - Bug #17810

addr2line.c: Some symbol names missing in C backtrace with Clang/LLVM

04/17/2021 06:44 AM - xtkoba (Tee KOBAYASHI)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		Backport: 2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN

Description

When Clang/LLVM is used for compilation, some symbol names are missing in C level backtrace information. An example:

```
-- C level backtrace information -----
(...snip...)
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_call_method_each_type+0x6a) [0x7f73856ac33f] ../vm_insnh
elper.c:3438
/var/tmp/ruby.debug/lib/libruby.so.3.1(0x7f73856ac29a) [0x7f73856ac29a]
/var/tmp/ruby.debug/lib/libruby.so.3.1(0x7f73856aadf6) [0x7f73856aadf6]
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_exec_core+0xff7) [0x7f738569c3cd] ../insns.def:792
/var/tmp/ruby.debug/lib/libruby.so.3.1(rb_vm_exec+0x5c9) [0x7f73856a78d4]
/var/tmp/ruby.debug/lib/libruby.so.3.1(rb_ec_exec_node+0xe5) [0x7f73855a1bec] ../eval.c:320
/var/tmp/ruby.debug/lib/libruby.so.3.1(ruby_run_node+0x5a) [0x7f73855a1acf] ../eval.c:379
/var/tmp/ruby.debug/bin/ruby(main+0x73) [0x55c15877ac4b] ../main.c:47
```

This seems to happen because dladdr(3) sometimes fills NULL in dli_sname which is then overwritten to lines[i].sname regardless of its previous value.

A patch is attached to fix this issue. It modifies addr2line.c so that it does not use dli_sname (and also dli_fname) when the value is NULL.

I also attach another patch that makes addr2line.c print source filename even when source lineno is not available (which is the case for rb_vm_exec in the above example).

When these two patches are applied, C level backtrace information is printed as follows.

```
-- C level backtrace information -----
(...snip...)
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_call_method_each_type+0x6a) [0x7fb08928231f] ../vm_insnh
elper.c:3438
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_call_method+0xf6) [0x7fb08928227a] ../vm_insnhelper.c:0
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_sendish+0x334) [0x7fb089280dd6] ../vm_insnhelper.c:0
/var/tmp/ruby.debug/lib/libruby.so.3.1(vm_exec_core+0xff7) [0x7fb0892723ad] ../insns.def:792
/var/tmp/ruby.debug/lib/libruby.so.3.1(rb_vm_exec+0x5c9) [0x7fb08927d8b4] ../vm.c:0
/var/tmp/ruby.debug/lib/libruby.so.3.1(rb_ec_exec_node+0xe5) [0x7fb089177bcc] ../eval.c:320
/var/tmp/ruby.debug/lib/libruby.so.3.1(ruby_run_node+0x5a) [0x7fb089177aaf] ../eval.c:379
/var/tmp/ruby.debug/bin/ruby(main+0x73) [0x557ed1e0bc4b] ../main.c:47
```

Associated revisions

Revision 940c8b093de1d903b67b7d80cc33f698a5debf1c - 06/09/2022 11:43 AM - xtkoba (Tee KOBAYASHI)

Skip NULL values from dladdr(3)

Fixes [Bug #17810]

Revision 940c8b093de1d903b67b7d80cc33f698a5debf1c - 06/09/2022 11:43 AM - xtkoba (Tee KOBAYASHI)

Skip NULL values from dladdr(3)

Fixes [Bug #17810]

Revision 940c8b09 - 06/09/2022 11:43 AM - xtkoba (Tee KOBAYASHI)

Skip NULL values from dladdr(3)

Fixes [Bug #17810]

History

#1 - 04/30/2021 02:11 PM - xtkoba (Tee KOBAYASHI)

PR: <https://github.com/ruby/ruby/pull/4438>

The second patch is omitted from the PR, because it turns out to be not very useful. The corresponding source file name should be easily guessable from the symbol name.

#2 - 06/09/2022 04:46 PM - xtkoba (Tee KOBAYASHI)

- Status changed from Open to Closed

Applied in changeset [git|940c8b093de1d903b67b7d80cc33f698a5debf1c](https://github.com/ruby/ruby/commit/940c8b093de1d903b67b7d80cc33f698a5debf1c).

Skip NULL values from dladdr(3)

Fixes [Bug [#17810](#)]

Files

ruby-addr2line-do-not-overwrite-sname-with-null.patch	1.07 KB	04/17/2021	xtkoba (Tee KOBAYASHI)
ruby-addr2line-print-filename-without-lineno.patch	574 Bytes	04/17/2021	xtkoba (Tee KOBAYASHI)