Ruby - Bug #20072

free(): invalid pointer when compiled with --enable-shared --with-jemalloc

12/18/2023 08:09 PM - misdoro (Mikhail Doronin)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	3.3		
ruby -v:	ruby 3.3.0dev (2023-08-17T01:57:09Z test 5bb9462285) [x86_64-linux]	**Backport:**	3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN

Description

When ruby is built with --enable-shared --with-jemalloc on Linux (current Gentoo, ubuntu22 in docker),

running a rails app yields:

```
free(): invalid pointer
Aborted
```

The issue started appearing after 5bb946228550c7f171c27725860b153a675404f3
https://github.com/ruby/ruby/commit/5bb946228550c7f171c27725860b153a675404f3

Related to https://bugs.ruby-lang.org/issues/18409 (workaround to LD_PRELOAD jemalloc from that issue works)

Related issues:

Related to Ruby - Bug #19831: warning message of linker with macOS Sonoma beta	**Open**

History

#1 - 12/19/2023 03:21 AM - nobu (Nobuyoshi Nakada)

Could you share your config.log and crash report?

#2 - 12/19/2023 06:52 AM - hsbt (Hiroshi SHIBATA)

- Target version set to 3.3

#3 - 12/19/2023 05:07 PM - misdoro (Mikhail Doronin)

- File config.log added

Hi Nobu, you will find the config.log attached.

Debugged it a bit deeper, it boils down to:

- install ruby with --enable-shared --with-jemalloc
- gem install sassc
- running irb and require 'sassc'
  that is immediately crashing:

```
$ irb
irb(main):001> require 'sassc'
free(): invalid pointer
Aborted
```

#4 - 12/20/2023 04:13 AM - kjtsanaktsidis (KJ Tsanaktsidis)

I wasn't able to reproduce your crash, but there is definitely a problem - when using --enable-shared and --with-jemalloc together, the Ruby that gets built still uses libc's malloc and ignores jemalloc. This is because we pass -ljemalloc to the link line for libruby.so, but we *don't* pass it to ruby. This means that the built Ruby isn't marked as needing libjemalloc.so:

```
root@jammy-189dc9d584290f1a:/var/ruby# readelf --dynamic ruby | grep NEEDED
 0x0000000000000001 (NEEDED)             Shared library: [libruby.so.3.3]
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
```

And because the dynamic linker (at least the glibc one) links libraries in breadth-first order, that means that libc.so.6 is linked before libjemalloc.so.2:

```
root@jammy-189dc9d584290f1a:/var/ruby# ldd ruby
```

```
linux-vdso.so.1 (0x00007ffe873fb000)
libruby.so.3.3 => /usr/local/lib/libruby.so.3.3 (0x00007f8870000000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f886fc00000)
libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f887054c000)
libjemalloc.so.2 => /lib/x86_64-linux-gnu/libjemalloc.so.2 (0x00007f886f800000)
libcrypt.so.1 => /lib/x86_64-linux-gnu/libcrypt.so.1 (0x00007f8870512000)
libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007f886ff19000)
/lib64/ld-linux-x86-64.so.2 (0x00007f8870572000)
libstdc++.so.6 => /lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007f886f400000)
libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007f886fef9000)
```

We need to pass -ljemalloc to the linker command line for the final Ruby executable. I'm playing around trying to find the right Autoconf magic spells for this now.

#5 - 12/20/2023 04:51 AM - hsbt (Hiroshi SHIBATA)

- Related to Bug #19831: warning message of linker with macOS Sonoma beta added

#6 - 12/20/2023 04:52 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Open to Closed

https://github.com/ruby/ruby/pull/9284 has been merged.

#19831 is already solved. There are no warnings with the latest Xcode.

#7 - 12/20/2023 05:10 AM - shyouhei (Shyouhei Urabe)

This issue reminds me of https://github.com/ruby/ruby/pull/4627

#8 - 12/20/2023 12:28 PM - misdoro (Mikhail Doronin)

- File deleted (config.log)