

Ruby - Bug #15852

APPLICATION_VERIFIER_LOCKS_LOCK_IN_FREED_HEAP on exiting ruby

05/15/2019 09:05 PM - test35965@gmail.com (Alexander Riccio)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.6.3p62 (2019-04-16 revision 67580) [x64-mingw32]	Backport: 2.6: DONE, 2.7: DONE, 3.0: DONE
Description Ruby appears to be freeing some critical section in ruby_vm_destruct before deleting the critical section. Critical Section objects must be deleted with DeleteCriticalSection (https://docs.microsoft.com/en-us/windows/desktop/api/synchapi/nf-synchapi-deletecriticalsection) before freeing the owning memory. I can't tell exactly what critical section is being freed - I'm new to ruby, don't know how the VM works, and haven't built it locally - so I can't help you guys there yet. The clean stack trace is: <pre>0:000> kc # Call Site 00 vrfcore!VerifierStopMessageEx 01 vfbasics!AVrfpFreeMemLockChecks 02 vfbasics!AVrfpFreeMemNotify 03 vfbasics!AVrfpRtlFreeHeap 04 msvcrtd!free 05 vfbasics!AVrfp_free 06 x64_msvcrtd_ruby260!ruby_xfree 07 x64_msvcrtd_ruby260!ruby_vm_destruct 08 x64_msvcrtd_ruby260!ruby_cleanup 09 x64_msvcrtd_ruby260!ruby_run_node 0a image00000000_00400000 0b image00000000_00400000 0c image00000000_00400000 0d KERNEL32!BaseThreadInitThunk 0e ntdll!RtlUserThreadStart</pre> I'm running C:\Ruby26-x64\bin\ruby.exe -x "C:\Ruby26-x64\bin\irb.cmd" , with Application Verifier lock verification enabled. Application Verifier is the Windows SDK dynamic analysis tool, and it can be enabled by anybody who's installed the SDK. Add ruby.exe to the list of applications in Application Verifier and then run irb from inside windbg. Leak analysis should be enabled by default. I've attached the full debug log in Windbg.		

Associated revisions

Revision 2a83650b0fd25719fb6c03bfec7bd895734d3ceb - 03/09/2021 11:11 AM - nobu (Nobuyoshi Nakada)

Destroy VM-wise locks before freeing [Bug #15852]

Revision 2a83650b0fd25719fb6c03bfec7bd895734d3ceb - 03/09/2021 11:11 AM - nobu (Nobuyoshi Nakada)

Destroy VM-wise locks before freeing [Bug #15852]

Revision 2a83650b - 03/09/2021 11:11 AM - nobu (Nobuyoshi Nakada)

Destroy VM-wise locks before freeing [Bug #15852]

Revision 0074ea2d83230e10ab0cd769fff203c13d3c592f - 03/11/2021 11:06 AM - naruse (Yui NARUSE)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 0074ea2d83230e10ab0cd769fff203c13d3c592f - 03/11/2021 11:06 AM - naruse (Yui NARUSE)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 0074ea2d - 03/11/2021 11:06 AM - naruse (Yui NARUSE)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 30942fc4d89a04792e9eba7d3c4e5009c54e81da - 03/20/2021 03:49 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 30942fc4d89a04792e9eba7d3c4e5009c54e81da - 03/20/2021 03:49 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 30942fc4 - 03/20/2021 03:49 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

```
---
thread.c | 7 -----
vm.c     | 2 ++
2 files changed, 2 insertions(+), 7 deletions(-)
```

Revision 5f83e778cc6cfe5982f73e3296286472b84a147 - 04/04/2021 11:50 PM - U.Nakamura

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67930 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 5f83e778cc6cfe5982f73e3296286472b84a147 - 04/04/2021 11:50 PM - U.Nakamura

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67930 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

merge revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb: [Backport #15852]

Destroy VM-wise locks before freeing [Bug #15852]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67930 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 05/15/2019 09:52 PM - test35965@gmail.com (Alexander Riccio)

Uhh, I don't know how to add maintainers, sorry!

#2 - 02/08/2021 08:03 PM - test35965@gmail.com (Alexander Riccio)

Still active as of Ruby 3.0.0p0 (x64-mingw32). I've done some more digging, and it appears to be freeing the Thread_Mutex in rb_call_inits (inits.c), aka the Init_Thread_Mutex function in thread.c.

#3 - 02/08/2021 08:08 PM - test35965@gmail.com (Alexander Riccio)

How do I assign? It looks like this should go to [@ko1 \(Koichi Sasada\)](#) (eval) or [@nobu \(Nobuyoshi Nakada\)](#) (mingw)

#4 - 02/19/2021 03:04 AM - nobu (Nobuyoshi Nakada)

vm->waitpid_lock and vm->workqueue_lock seem never deleted.
rb_native_mutex_destroy on them are disabled by if (0) in rb_vm_gvl_destroy(), and that function is not called from anywhere too.
I have no idea why these calls are disabled.

<https://github.com/nobu/ruby/tree/bug/15852-delete-critsec>

#5 - 03/09/2021 11:11 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset [git|2a83650b0fd25719fb6c03bfec7bd895734d3ceb](#).

Destroy VM-wise locks before freeing [Bug [#15852](#)]

#6 - 03/11/2021 12:57 AM - nobu (Nobuyoshi Nakada)

- Backport changed from 2.4: UNKNOWN, 2.5: UNKNOWN, 2.6: UNKNOWN to 2.6: REQUIRED, 2.7: REQUIRED, 3.0: REQUIRED

vm->waitpid_lock and vm->workqueue_lock seem never deleted.
rb_native_mutex_destroy on them are disabled by if (0) in rb_vm_gvl_destroy(), and that function is not called from anywhere too.
I have no idea why these calls are disabled.

#7 - 03/11/2021 11:06 AM - naruse (Yui NARUSE)

- Backport changed from 2.6: REQUIRED, 2.7: REQUIRED, 3.0: REQUIRED to 2.6: REQUIRED, 2.7: REQUIRED, 3.0: DONE

ruby_3_0 0074ea2d83230e10ab0cd769fff203c13d3c592f merged revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb.

#8 - 03/20/2021 04:19 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.6: REQUIRED, 2.7: REQUIRED, 3.0: DONE to 2.6: REQUIRED, 2.7: DONE, 3.0: DONE

ruby_2_7 30942fc4d89a04792e9eba7d3c4e5009c54e81da merged revision(s) 2a83650b0fd25719fb6c03bfec7bd895734d3ceb.

#9 - 04/04/2021 11:51 PM - usa (Usaku NAKAMURA)

- Backport changed from 2.6: REQUIRED, 2.7: DONE, 3.0: DONE to 2.6: DONE, 2.7: DONE, 3.0: DONE

backported into ruby_2_6 at r67930

Files

ruby_freeing_active_critsec.TXT	17.2 KB	05/15/2019	test35965@gmail.com (Alexander Riccio)
---------------------------------	---------	------------	--