Ruby master - Bug #14667

Segmentation fault in Ruby during iOS automation

04/06/2018 12:22 AM - sankalp89 (Sankalp Anand)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	2.3.1 p112	**Backport:**	2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN

Description

Hello,

I'm using Calabash for iOS automation. My tests are crashing the ruby interpreter. Could you please help in finding out what the issue is?

Best,
Sankalp

```
[u"Running with options: '14e26a69f942dd7867bc33c547b8924684c916d0 com.cisco.squared.sqbudev /User
s/testmaskin/Wx2/wx2-ios-client/build/WebExSquaredIntegrationTests.ipa'\n"
 ** \x1b[1;95m14e26a69f942dd7867bc33c547b8924684c916d0: Requesting uninstallation of\x1b[0m: \x1b[
1;34mcom.apple.test.DeviceAgent-Runner\x1b[0m
 \x1b[1;34m[ ***** ideviceinstaller -u 14e26a69f942dd7867bc33c547b8924684c916d0 -U com.apple.test.
DeviceAgent-Runner -d]\x1b[0m
u"\x1b[1;47mUninstalling 'com.apple.test.DeviceAgent-Runner'\x1b[0m\n"
 \x1b[1;47m- RemovingApplication (50%)\x1b[0m
 \x1b[1;47m- Complete\x1b[0m
 ** \x1b[1;95m14e26a69f942dd7867bc33c547b8924684c916d0: Requesting uninstallation of\x1b[0m: \x1b[
1;34mcom.cisco.squared.sqbudev\x1b[0m
 \x1b[1;34m[ ***** ideviceinstaller -u 14e26a69f942dd7867bc33c547b8924684c916d0 -U com.cisco.squar
ed.sqbudev -d]\x1b[0m
u"\x1b[1;47mUninstalling 'com.cisco.squared.sqbudev'\x1b[0m\n"
 \x1b[1;47m- RemovingApplication (50%)\x1b[0m
 \x1b[1;47m- GeneratingApplicationMap (90%)\x1b[0m
 \x1b[1;47m- Complete\x1b[0m
 ** \x1b[1;95minstalling app from\x1b[0m: \x1b[1;34mPublicStaging/WebExSquaredIntegrationTests.ipa
\x1b[0m
 ** \x1b[1;95mUploading /Users/testmaskin/Wx2/wx2-ios-client/build/WebExSquaredIntegrationTests.ip
a to\x1b[0m: \x1b[1;34mPublicStaging/WebExSquaredIntegrationTests.ipa\x1b[0m
 \x1b[1;34m[ ***** xcrun xcodebuild -version]\x1b[0m
(snip)
  ]
```

History

#1 - 04/06/2018 07:21 AM - sankalp89 (Sankalp Anand)

This is the crash dump from /Library/Logs/CrashReporter/

```
Process:               ruby [59453]
Path:                  /Users/USER/*/ruby
Identifier:            ruby
Version:               0
Code Type:             X86-64 (Native)
Parent Process:        sshd [58859]
Responsible:           ruby [59453]
User ID:               501

Date/Time:             2018-04-06 01:12:35.551 -0700
OS Version:            Mac OS X 10.12.6 (16G29)
Report Version:        12
Anonymous UUID:        9FF3048A-7854-9BA5-8EA7-25F5AA871E27
```

```
Time Awake Since Boot: 30000 seconds

System Integrity Protection: enabled

Crashed Thread:        5

Exception Type:        EXC_BAD_ACCESS (SIGABRT)
Exception Codes:       KERN_INVALID_ADDRESS at 0x0000000000002000
Exception Note:        EXC_CORPSE_NOTIFY

VM Regions Near 0x2000:
-->
    __TEXT                 0000000106a66000-0000000106c9d000 [ 2268K] r-x/rwx SM=COW  /Users/USER/*

Application Specific Information:
abort() called

Thread 0:: Dispatch queue: com.apple.main-thread
0   libsystem_kernel.dylib          0x0000000107f6e246 read + 10
1   ruby                            0x0000000106c0f7ec rb_thread_io_blocking_region + 188
2   ruby                            0x0000000106ade925 io_fillbuf + 149
3   ruby                            0x0000000106adf792 rb_io_getline_1 + 2610
4   ruby                            0x0000000106ae8b4c rb_io_gets_m + 44
5   ruby                            0x0000000106bfdaf6 vm_call_cfunc + 278
6   ruby                            0x0000000106be8a58 vm_exec_core + 9784
7   ruby                            0x0000000106bf858f vm_exec + 127
8   ruby                            0x0000000106ab2e18 ruby_exec_internal + 152
9   ruby                            0x0000000106ab2d26 ruby_run_node + 54
10  ruby                            0x0000000106a66f0f main + 79
11  libdyld.dylib                   0x0000000107d8a235 start + 1

Thread 1:: ruby-timer-thr
0   libsystem_kernel.dylib          0x0000000107f6e19e poll + 10
1   ruby                            0x0000000106c15ca3 thread_timer + 371
2   libsystem_pthread.dylib         0x00000001080d093b _pthread_body + 180
3   libsystem_pthread.dylib         0x00000001080d0887 _pthread_start + 286
4   libsystem_pthread.dylib         0x00000001080d008d thread_start + 13

Thread 2:
0   libsystem_kernel.dylib          0x0000000107f6cbf2 __psynch_cvwait + 10
1   libsystem_pthread.dylib         0x00000001080d17fa _pthread_cond_wait + 712
2   ffi_c.bundle                    0x000000010841311b async_cb_wait + 91
3   ruby                            0x0000000106c0f6a5 rb_thread_call_without_gvl + 85
4   ffi_c.bundle                    0x0000000108412703 async_cb_event + 67
5   ruby                            0x0000000106c156d4 thread_start_func_2 + 660
6   ruby                            0x0000000106c1541a thread_start_func_1 + 170
7   libsystem_pthread.dylib         0x00000001080d093b _pthread_body + 180
8   libsystem_pthread.dylib         0x00000001080d0887 _pthread_start + 286
9   libsystem_pthread.dylib         0x00000001080d008d thread_start + 13

Thread 3:
0   libsystem_kernel.dylib          0x0000000107f6cbf2 __psynch_cvwait + 10
1   libsystem_pthread.dylib         0x00000001080d17fa _pthread_cond_wait + 712
2   ffi_c.bundle                    0x000000010841287b callback_invoke + 331
3   libffi.dylib                    0x0000000107c55a2a ffi_closure_unix64_inner + 502
4   libffi.dylib                    0x0000000107c5509e ffi_closure_unix64 + 70
5   libimobiledevice.dylib          0x000000010843dba7 instproxy_receive_status_loop + 354
6   libimobiledevice.dylib          0x000000010843d9f2 instproxy_receive_status_loop_thread + 29
7   libsystem_pthread.dylib         0x00000001080d093b _pthread_body + 180
8   libsystem_pthread.dylib         0x00000001080d0887 _pthread_start + 286
9   libsystem_pthread.dylib         0x00000001080d008d thread_start + 13

Thread 4:
0   libsystem_kernel.dylib          0x0000000107f6d3ee __wait4 + 10
1   ruby                            0x0000000106b38e79 rb_waitpid_blocking + 25
2   ruby                            0x0000000106c0f6a5 rb_thread_call_without_gvl + 85
3   ruby                            0x0000000106b30d89 rb_waitpid + 73
4   ruby                            0x0000000106b30f0c detach_process_watcher + 44
5   ruby                            0x0000000106c156d4 thread_start_func_2 + 660
6   ruby                            0x0000000106c1541a thread_start_func_1 + 170
7   libsystem_pthread.dylib         0x00000001080d093b _pthread_body + 180
8   libsystem_pthread.dylib         0x00000001080d0887 _pthread_start + 286
9   libsystem_pthread.dylib         0x00000001080d008d thread_start + 13

Thread 5 Crashed:
```

```
0   libsystem_kernel.dylib          0x0000000107f6cd42 __pthread_kill + 10
1   libsystem_pthread.dylib         0x00000001080d3457 pthread_kill + 90
2   libsystem_c.dylib               0x0000000107e67420 abort + 129
3   ruby                            0x0000000106aaa329 die + 9
4   ruby                            0x0000000106aaa54a rb_bug_context + 538
5   ruby                            0x0000000106b7be54 sigsegv + 68
6   libsystem_platform.dylib        0x00000001080beb3a _sigtramp + 26

Thread 5 crashed with X86 Thread State (64-bit):
  rax: 0x0000000000000000  rbx: 0x0000000000000006  rcx: 0x00007f852e1fa808  rdx: 0x0000000000000000
  rdi: 0x0000000000001503  rsi: 0x0000000000000006  rbp: 0x00007f852e1fa830  rsp: 0x00007f852e1fa808
   r8: 0x0000000000000040   r9: 0x0000000107e9a040  r10: 0x0000000008000000  r11: 0x0000000000000202
  r12: 0x00007f852e1fa880  r13: 0x0000000000000000  r14: 0x000070000b9b2000  r15: 0x0000000106c2c3d6
  rip: 0x0000000107f6cd42  rfl: 0x0000000000000202  cr2: 0x0000000106cebf2a

Logical CPU:     0
Error Code:      0x02000148
Trap Number:     133


Binary Images:
       0x106a66000 -        0x106c9cff3 +ruby (0) <F5D9E742-4A96-3422-9341-3E911A61B9DF> /Users/USER/*/ruby
       0x106cfb000 -        0x107194ff7  com.apple.CoreFoundation (6.9 - 1349.8) <09ED473E-5DE8-307F-B55C-16F6
419236D5> /System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation
       0x107435000 -        0x107435fff +escape.bundle (0) <06B26EF3-943E-383E-AD56-6D832AB52916> /Users/USER/
*/escape.bundle
       0x107438000 -        0x107439ffb  libSystem.B.dylib (1238.60.2) <F18AC1E7-C6F1-34B1-8069-BE571B3231D4>
/usr/lib/libSystem.B.dylib
       0x107440000 -        0x107812047  libobjc.A.dylib (709.1) <70614861-0340-32E2-85ED-FE65759CDFFA> /usr/l
ib/libobjc.A.dylib
       0x1078f0000 -        0x1078f1ffb +encdb.bundle (0) <8D4CFBCE-30F8-324A-A9CE-B002DA2D99ED> /Users/USER/*
/encdb.bundle
       0x1078f4000 -        0x1078f5ff3  libDiagnosticMessagesClient.dylib (102) <84A04D24-0E60-3810-A8C0-90A6
5E2DF61A> /usr/lib/libDiagnosticMessagesClient.dylib
       0x1078fb000 -        0x1078fcfff +transdb.bundle (0) <32CD7CCC-9126-3784-8A6B-22BE5B664A94> /Users/USER
/*/transdb.bundle
       0x107900000 -        0x107b25ffb  libicucore.A.dylib (57166.0.1) <CCD2ED24-3071-383B-925D-8D763BB12A6F>
 /usr/lib/libicucore.A.dylib
       0x107bf9000 -        0x107c0aff3  libz.1.dylib (67) <46E3FFA2-4328-327A-8D34-A03E20BFFB8E> /usr/lib/lib
z.1.dylib
       0x107c10000 -        0x107c11ff7 +console.bundle (0) <852C7A0F-F690-35C3-A1E7-60701403990C> /Users/USER
/*/console.bundle
       0x107c17000 -        0x107c1bff7  libcache.dylib (79) <093A4DAB-8385-3D47-A350-E20CB7CCF7BF> /usr/lib/s
ystem/libcache.dylib
       0x107c25000 -        0x107c2ffff  libcommonCrypto.dylib (60092.50.5) <8A64D1B0-C70E-385C-92F0-E669079FD
A90> /usr/lib/system/libcommonCrypto.dylib
       0x107c3f000 -        0x107c46fff  libcompiler_rt.dylib (62) <55D47421-772A-32AB-B529-1A46C2F43B4D> /usr
/lib/system/libcompiler_rt.dylib
       0x107c54000 -        0x107c55fff  libffi.dylib (18.1) <49D03682-E111-351C-8266-4519B3B82BE9> /usr/lib/l
ibffi.dylib
       0x107c5a000 -        0x107c62fff  libcopyfile.dylib (138) <819BEA3C-DF11-3E3D-A1A1-5A51C5BF1961> /usr/l
ib/system/libcopyfile.dylib
       0x107c6d000 -        0x107cf0fdf  libcorecrypto.dylib (442.50.19) <65D7165E-2E71-335D-A2D6-33F78E2DF0C1
> /usr/lib/system/libcorecrypto.dylib
       0x107d0c000 -        0x107d0fff7 +etc.bundle (0) <99646534-A6B1-30D3-9E42-4761C09C5404> /Users/USER/*/e
tc.bundle
       0x107d13000 -        0x107d44fff  libdispatch.dylib (703.50.37) <6582BAD6-ED27-3B30-B620-90B1C5A4AE3C>
/usr/lib/system/libdispatch.dylib
       0x107d85000 -        0x107d8affb  libdyld.dylib (433.5) <9B2AC56D-107C-3541-A127-9094A751F2C9> /usr/lib
/system/libdyld.dylib
       0x107d95000 -        0x107d95ffb  libkeymgr.dylib (28) <7AA011A9-DC21-3488-BF73-3B5B14D1FDD6> /usr/lib/
system/libkeymgr.dylib
       0x107da0000 -        0x107da0fff  liblaunch.dylib (972.70.1) <B856ABD2-896E-3DE0-B2C8-146A6AF8E2A7> /us
r/lib/system/liblaunch.dylib
       0x107daf000 -        0x107db4ff3  libmacho.dylib (898) <17D5D855-F6C3-3B04-B680-E9BF02EF8AED> /usr/lib/
system/libmacho.dylib
       0x107dbd000 -        0x107dbfff3  libquarantine.dylib (85.50.1) <12448CC2-378E-35F3-BE33-9DC395A5B970>
/usr/lib/system/libquarantine.dylib
       0x107dc7000 -        0x107dc8ffb  libremovefile.dylib (45) <38D4CB9C-10CD-30D3-8B7B-A515EC75FE85> /usr/
lib/system/libremovefile.dylib
       0x107dd4000 -        0x107decff7  libsystem_asl.dylib (349.50.5) <096E4228-3B7C-30A6-8B13-EC909A64499A>
 /usr/lib/system/libsystem_asl.dylib
       0x107e01000 -        0x107e01ff7  libsystem_blocks.dylib (67) <10DC5404-73AB-35B3-A277-A8AFECB476EB> /u
sr/lib/system/libsystem_blocks.dylib
       0x107e08000 -        0x107e95fef  libsystem_c.dylib (1158.50.2) <E5AE5244-7D0C-36AC-8BB6-C7AE7EA52A4B>
```

```
/usr/lib/system/libsystem_c.dylib
       0x107ec0000 -        0x107ec3ffb  libsystem_configuration.dylib (888.60.2) <BECC01A2-CA8D-31E6-BCDF-D45
2965FA976> /usr/lib/system/libsystem_configuration.dylib
       0x107ece000 -        0x107ed1fff  libsystem_coreservices.dylib (41.4) <7D26DE79-B424-3450-85E1-F7FAB327
14AB> /usr/lib/system/libsystem_coreservices.dylib
       0x107edc000 -        0x107ef4fff  libsystem_coretls.dylib (121.50.4) <EC6FCF07-DCFB-3A03-9CC9-6DD370997
4C6> /usr/lib/system/libsystem_coretls.dylib
       0x107f00000 -        0x107f06fff  libsystem_dnssd.dylib (765.50.9) <CC960215-0B1B-3822-A13A-3DDE96FA796
F> /usr/lib/system/libsystem_dnssd.dylib
       0x107f11000 -        0x107f3aff7  libsystem_info.dylib (503.50.4) <611DB84C-BF70-3F92-8702-B9F28A900920
> /usr/lib/system/libsystem_info.dylib
       0x107f53000 -        0x107f75ff7  libsystem_kernel.dylib (3789.70.16) <34B1F16C-BC9C-3C5F-9045-0CAE91CB
5914> /usr/lib/system/libsystem_kernel.dylib
       0x107f8f000 -        0x107fd6fe7  libsystem_m.dylib (3121.6) <86D499B5-BBDC-3D3B-8A4E-97AE8E6672A4> /us
r/lib/system/libsystem_m.dylib
       0x107fe3000 -        0x108001ff7  libsystem_malloc.dylib (116.50.8) <A3D15F17-99A6-3367-8C7E-4280E8619C
95> /usr/lib/system/libsystem_malloc.dylib
       0x108015000 -        0x10806effb  libsystem_network.dylib (856.60.1) <369D0221-56CA-3C3E-9EDE-94B41CAE7
7B7> /usr/lib/system/libsystem_network.dylib
       0x108093000 -        0x10809cff3  libsystem_networkextension.dylib (563.60.2) <B021F2B3-8A75-3633-ABB0-
FC012B8E9B0C> /usr/lib/system/libsystem_networkextension.dylib
       0x1080aa000 -        0x1080b3ff3  libsystem_notify.dylib (165.20.1) <B8160190-A069-3B3A-BDF6-2AA408221F
AE> /usr/lib/system/libsystem_notify.dylib
       0x1080bc000 -        0x1080c4fe7  libsystem_platform.dylib (126.50.8) <897462FD-B318-321B-A554-E6198263
0F7E> /usr/lib/system/libsystem_platform.dylib
       0x1080cd000 -        0x1080d7ff7  libsystem_pthread.dylib (218.60.3) <B8FB5E20-3295-39E2-B5EB-B464D1D4B
104> /usr/lib/system/libsystem_pthread.dylib
       0x1080e4000 -        0x1080e7ff7  libsystem_sandbox.dylib (592.70.1) <4B92EC49-ACD0-36AE-B07A-A2B8152EA
F9D> /usr/lib/system/libsystem_sandbox.dylib
       0x1080ee000 -        0x1080efff3  libsystem_secinit.dylib (24.50.4) <F78B847B-3565-3E4B-98A6-F7AD40392E
2D> /usr/lib/system/libsystem_secinit.dylib
       0x1080fc000 -        0x108103ffb  libsystem_symptoms.dylib (532.50.47) <3390E07C-C1CE-348F-ADBD-2C5440B
45EAA> /usr/lib/system/libsystem_symptoms.dylib
       0x108110000 -        0x108123ff7  libsystem_trace.dylib (518.70.1) <AC63A7FE-50D9-3A30-96E6-F6B7FF16E46
5> /usr/lib/system/libsystem_trace.dylib
       0x108135000 -        0x10813affb  libunwind.dylib (35.3) <3D50D8A8-C460-334D-A519-2DA841102C6B> /usr/li
b/system/libunwind.dylib
       0x108148000 -        0x108171ff7  libxpc.dylib (972.70.1) <BF896DF0-D8E9-31A8-A4B3-01120BFEEE52> /usr/l
ib/system/libxpc.dylib
       0x108191000 -        0x1081baff7  libc++abi.dylib (307.4) <BC271AD3-831B-362A-9DA7-E8C51F285FE4> /usr/l
ib/libc++abi.dylib
       0x1081cc000 -        0x108222ff7  libc++.1.dylib (307.5) <0B43BB5D-E6EB-3464-8DE9-B41AC8ED9D1C> /usr/li
b/libc++.1.dylib
       0x1083ae000 -        0x1083b2fff +stringio.bundle (0) <BBF77ADB-BE98-3979-9FD7-780BFBDB1DCA> /Users/USE
R/*/stringio.bundle
       0x1083b7000 -        0x1083bcffb +pathname.bundle (0) <0BFB1C24-4E5C-329A-8FCA-1F0BA6CC36DF> /Users/USE
R/*/pathname.bundle
       0x1083c1000 -        0x1083f6fff +date_core.bundle (0) <BE52A6F1-22FB-3780-85D4-36D5C9F377A7> /Users/US
ER/*/date_core.bundle
       0x108407000 -        0x10841dfff +ffi_c.bundle (0) <5008718A-E6A7-34A1-8E81-F0C10AFDC803> /Users/USER/*
/ffi_c.bundle
       0x108428000 -        0x108430ff3 +libplist.dylib (0) <193A785C-82FF-3377-A7F7-B9E0299C3233> /usr/local/
lib/libplist.dylib
       0x108434000 -        0x108448fff +libimobiledevice.dylib (0) <04DAB5EE-2203-33F6-A84F-F923D71787BF> /us
r/local/lib/libimobiledevice.dylib
       0x108453000 -        0x108494fff +libssl.1.0.0.dylib (0) <3C28C2A8-036B-34B3-82BB-5780DB7271B2> /usr/lo
cal/opt/openssl/lib/libssl.1.0.0.dylib
       0x1084b3000 -        0x108623c87 +libcrypto.1.0.0.dylib (0) <1C6D06DA-0F88-37BA-80E9-52C4AC7E942C> /usr
/local/opt/openssl/lib/libcrypto.1.0.0.dylib
       0x10869d000 -        0x1086a1fff +libusbmuxd.4.dylib (0) <68265A3E-31C5-32E7-8170-D6E81FF2E021> /usr/lo
cal/opt/usbmuxd/lib/libusbmuxd.4.dylib
       0x1111ac000 -        0x1111e9dc7  dyld (433.5) <322C06B7-8878-311D-888C-C8FD2CA96FF3> /usr/lib/dyld

External Modification Summary:
  Calls made by other processes targeting this process:
    task_for_pid: 0
    thread_create: 0
    thread_set_state: 0
  Calls made by this process:
    task_for_pid: 0
    thread_create: 0
    thread_set_state: 0
  Calls made by all processes on this machine:
    task_for_pid: 11316
    thread_create: 0
```

```
    thread_set_state: 0

VM Region Summary:
ReadOnly portion of Libraries: Total=23.4M resident=0K(0%) swapped_out_or_unallocated=23.4M(100%)
Writable regions: Total=88.1M written=0K(0%) resident=0K(0%) swapped_out=0K(0%) unallocated=88.1M(100%)

                                VIRTUAL   REGION
REGION TYPE                        SIZE    COUNT (non-coalesced)
===========                     =======  =======
Kernel Alloc Once                    8K        2
MALLOC                            76.2M       16
MALLOC guard page                   16K        4
STACK GUARD                       56.0M        6
Stack                             11.6M        7
Stack Guard                          4K        2
VM_ALLOCATE                         12K        4
__DATA                            3256K       77
__LINKEDIT                        4404K       60
__TEXT                            19.1M       60
__UNICODE                           556K        2
shared memory                       12K        4
===========                     =======  =======
TOTAL                             170.9M      232
```

#2 - 04/06/2018 12:58 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Feedback

- Description updated

- File bug-14667.log added

```
-- C level backtrace information -------------------------------------------
0   ruby                                0x00000001022a610b rb_vm_bugreport + 379
1   ruby                                0x00000001021494ef rb_bug_context + 447
2   ruby                                0x000000010221ae54 sigsegv + 68
3   libsystem_platform.dylib            0x00007fff5a4d5f5a _sigtramp + 26
4   ruby                                0x0000000102246a53 rb_id_table_lookup + 115
5   ???                                 0x000070000240f9e0 0x0 + 123145340123616
```

The stack frame seems broken, maybe the last return address has been cleared partially?
It may be related to ffi.
How can I reproduce it, and does it occur with newer versions?

#3 - 04/06/2018 11:52 PM - sankalp89 (Sankalp Anand)

My automation tests are trying to install the iOS application-

ruby ~/path/to/install/script/install_ipa.rb com.company.squared.sqbudev ~/path/to/ipa/WebExSquaredIntegrationTests.ipa

#4 - 08/26/2019 07:35 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Feedback to Closed

Files

bug-14667.log	12.8 KB	04/06/2018	nobu (Nobuyoshi Nakada)