Ruby trunk - Bug #14261

invalid syntax segfaults: "x, true"

12/30/2017 10:19 PM - normalperson (Eric Wong)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE

Description

The `item' arg passed to list_append_gen is NULL, so it segfaults.
It happens on both x86 (32-bit) and x86-64 Linux.
I'm not familiar with the parser, so I will let a parser expert fix this.

```
./miniruby -e "x, true"

-e:1: Can't assign to true
x, true
       ^
./miniruby: [BUG] Segmentation fault at 0x00000010
ruby 2.6.0dev (2017-12-31 trunk 61519) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0001 p:0000 s:0003 E:001f48 (none) [FINISH]


-- Machine register context ------------------------------------------------
  GS: 0x00000063  FS: 0x00000000  ES: 0x0000002b  DS: 0x0000002b EDI: 0x56f02758
 ESI: 0x56f02778 EBP: 0x00000000 ESP: 0xff9cc640 EBX: 0x569dbb94 EDX: 0x00000000
 ECX: 0x00000003 EAX: 0x56f02778 TRA: 0x0000000e ERR: 0x00000004 EIP: 0x567703a4
  CS: 0x00000023 EFL: 0x00010206 UES: 0xff9cc640  SS: 0x0000002b

-- C level backtrace information -------------------------------------------
/path/to/ruby/miniruby(rb_vm_bugreport+0x4b0) [0x56880660] vm_dump.c:703
/path/to/ruby/miniruby(rb_bug_context+0x62) [0x566e7782] error.c:580
/path/to/ruby/miniruby(sigsegv+0x49) [0x567e9559] signal.c:928
linux-gate.so.1(0xf777ecc0) [0xf777ecc0]
/path/to/ruby/miniruby(list_append_gen+0x74) [0x567703a4] parse.y:8957
/path/to/ruby/miniruby(ruby_yyparse+0x12a3e) [0x5678d4ae] parse.y:1807
/path/to/ruby/miniruby(yycompile0+0xf7) [0x5678d607] parse.y:5595
/path/to/ruby/miniruby(rb_suppress_tracing+0xcf) [0x5688440f] vm_trace.c:397
/path/to/ruby/miniruby(rb_parser_compile_string+0xde) [0x56775cae] parse.y:5637
/path/to/ruby/miniruby(process_options+0x9e1) [0x567e7e61] ruby.c:1677
/path/to/ruby/miniruby(ruby_process_options+0x132) [0x567e8c42] ruby.c:2257
/path/to/ruby/miniruby(ruby_options+0xa7) [0x566f14d7] eval.c:105
/path/to/ruby/miniruby(main+0x6c) [0x5666d5bc] ./main.c:42
```

Related issues:

Related to Ruby trunk - Bug #14796: improper passing of &block - causes crash...	**Closed**
Has duplicate Ruby trunk - Bug #14361: Segmentation fault when array includes...	**Closed**
Has duplicate Ruby trunk - Bug #14544: crash on gem update	**Closed**
Has duplicate Ruby trunk - Bug #14554: gem update crashes	**Closed**
Has duplicate Ruby trunk - Bug #14620: Incorrect assignment causes segfault	**Closed**
Has duplicate Ruby trunk - Bug #14628: Misplaced colon causes segmentation fault	**Closed**
Has duplicate Ruby trunk - Bug #14627: class_eval "def foo(N:)\n end" regression	**Closed**
Has duplicate Ruby trunk - Bug #14911: Segmentation fault	**Rejected**

Associated revisions

Revision 45752157 - 12/31/2017 11:25 AM - nobu (Nobuyoshi Nakada)

parse.y: assignable_error

- parse.y (assignable_gen): should return valid NODE always even on errors. [ruby-core:84565] [Bug #14261]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61523 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61523 - 12/31/2017 11:25 AM - nobu (Nobuyoshi Nakada)

parse.y: assignable_error

- parse.y (assignable_gen): should return valid NODE always even on errors. [ruby-core:84565] [Bug #14261]

Revision 61523 - 12/31/2017 11:25 AM - nobu (Nobuyoshi Nakada)

parse.y: assignable_error

- parse.y (assignable_gen): should return valid NODE always even on errors. [ruby-core:84565] [Bug #14261]

Revision 2292ea6a - 02/21/2018 05:42 AM - naruse (Yui NARUSE)

merge revision(s) 61523: [Backport #14261]

```
parse.y: assignable_error

* parse.y (assignable_gen): should return valid NODE always even
  on errors.  [ruby-core:84565] [Bug #14261]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@62509 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 62509 - 02/21/2018 05:42 AM - naruse (Yui NARUSE)

merge revision(s) 61523: [Backport #14261]

```
parse.y: assignable_error

* parse.y (assignable_gen): should return valid NODE always even
  on errors.  [ruby-core:84565] [Bug #14261]
```

History

#1 - 12/31/2017 11:25 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset trunk|r61523.

---

parse.y: assignable_error

- parse.y (assignable_gen): should return valid NODE always even on errors. [ruby-core:84565] [Bug #14261]

#2 - 12/31/2017 11:50 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: REQUIRED

I can reproduce SEGV with 2.5.0.
I cannot reproduce with 2.4.3 but I cannot say with confidence that the recent changes cause the SEGV.
I'd like to do bisect when I have a time.

#3 - 01/09/2018 09:19 AM - vo.x (Vit Ondruch)

Thanks. Unfortunately, I cannot easily apply the patch into the tarball :/

#4 - 01/10/2018 02:40 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED

git bisect tell me that the SEGV was introduced by r60829 (https://github.com/ruby/ruby/commit/28d00c2fb2949c67f9510d61c41ad58047c4ab01).
After some exploration with debugger, it's obvious that the SEGV occured because item is NULL in list_append_gen().

Even though the cause of SEGV is not contained in 2.3/2.4, calling list_append_gen() with item=NULL should not be intended and buggy.
I will fill Backport field, but it is not so urgent for 2.3/2.4.
usa-san, please feel free to set WONTFIX. I think backporting r61523 is too difficult for such a trivial issue. I will take a look for ruby_2_4 later.

#5 - 01/18/2018 03:41 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14361: Segmentation fault when array includes two nil's without a comma between them: [nil nil, nil] added

#6 - 02/21/2018 05:42 AM - naruse (Yui NARUSE)

- Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE

ruby_2_5 r62509 merged revision(s) 61523.

#7 - 02/23/2018 03:57 PM - vo.x (Vit Ondruch)

- Has duplicate Bug #14544: crash on gem update added

#8 - 02/27/2018 02:25 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14554: gem update crashes added

#9 - 03/20/2018 02:53 PM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14620: Incorrect assignment causes segfault added

#10 - 03/24/2018 10:52 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14628: Misplaced colon causes segmentation fault added

#11 - 03/28/2018 07:06 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14627: class_eval "def foo(N:)\n end" regression added

#12 - 05/30/2018 07:57 AM - wanabe (_ wanabe)

- Related to Bug #14796: improper passing of &block - causes crash on MacOS 10.13.4 (17E202) with Ruby 2.5.0 within Rbenv added

#13 - 07/14/2018 04:24 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #14911: Segmentation fault added