

Ruby - Bug #19593

Crash due to throw data set as cause

04/12/2023 03:51 PM - peterzhu2118 (Peter Zhu)

Status:	Closed	Backport: 3.0: REQUIRED, 3.1: DONE, 3.2: DONE
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
Description		
GitHub PR: https://github.com/ruby/ruby/pull/7696		
rb_ec_setup_exception did not check if errno is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object. We saw a crash in show_cause due to id_cause of errno being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects. Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errno without checking if it is a throw_data.		
<pre>0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301bfa3f0, ctx=0x7f301bfa2c0) at signal.c:964 0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0 class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810 rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861 0x0000556c56f2f00f in show_cause (errno=errno@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, hi ghlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9 d1a2d68) at ./include/ruby/internal/special_consts.h:175</pre>		

Associated revisions

Revision 02a7e12b80823919fb614ad3ea6241d5115d14fe - 04/13/2023 12:38 PM - peterzhu2118 (Peter Zhu)

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errno is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errno being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errno without checking if it is a throw_data.

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301bfa3f0, ctx=0x7f301bfa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errno=errno@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```

Co-Authored-By: Jean Boussier byroot@ruby-lang.org

Revision 02a7e12b80823919fb614ad3ea6241d5115d14fe - 04/13/2023 12:38 PM - peterzhu2118 (Peter Zhu)

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errno is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errno being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errno without checking if it is a throw_data.

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301bfa3f0, ctx=0x7f301bfa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errno=errno@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```

Co-Authored-By: Jean Boussier byroot@ruby-lang.org

Revision 02a7e12b - 04/13/2023 12:38 PM - peterzhu2118 (Peter Zhu)

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errno is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errno being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errno without checking if it is a throw_data.

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301bfa3f0, ctx=0x7f301bfa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errno=errno@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```

Co-Authored-By: Jean Boussier byroot@ruby-lang.org

Revision 5fc9825ccf651664c547b1822c7f753464e27f06 - 07/17/2023 07:09 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errno is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errno being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errno without checking if it is a throw_data.

...

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301bfa3f0, ctx=0x7f301bfa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
```

```
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=
0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./includ
e/ruby/internal/special_consts.h:175
...

Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>
---
eval.c | 4 ++++
1 file changed, 4 insertions(+)
```

Revision 5fc9825ccf651664c547b1822c7f753464e27f06 - 07/17/2023 07:09 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errinfo is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errinfo being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errinfo without checking if it is a throw_data.

```
...
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=
0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./includ
e/ruby/internal/special_consts.h:175
...

Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>
---
eval.c | 4 ++++
1 file changed, 4 insertions(+)
```

Revision 5fc9825c - 07/17/2023 07:09 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errinfo is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errinfo being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errinfo without checking if it is a throw_data.

```
...
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
```

```
(errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```
```

Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>

---

eval.c | 4 ++++

1 file changed, 4 insertions(+)

## Revision c96ef4eee6b27796bb15ba161ef936998acbcf96 - 07/18/2023 11:50 AM - U.Nakamura

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb\_ec\_setup\_exception did not check if errinfo is a throw\_data. This can cause crashes in code since it is assumed that id\_cause is an object.

We saw a crash in show\_cause due to id\_cause of errinfo being a throw\_data. It crashes on rb\_obj\_is\_kind\_of since it cannot be called on T\_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb\_ec\_setup\_exception is the only place where id\_cause is assigned from errinfo without checking if it is a throw\_data.

```

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
```

```
(errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```
```

Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>

---

eval.c | 4 ++++

1 file changed, 4 insertions(+)

## Revision c96ef4eee6b27796bb15ba161ef936998acbcf96 - 07/18/2023 11:50 AM - U.Nakamura

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb\_ec\_setup\_exception did not check if errinfo is a throw\_data. This can cause crashes in code since it is assumed that id\_cause is an object.

We saw a crash in show\_cause due to id\_cause of errinfo being a throw\_data. It crashes on rb\_obj\_is\_kind\_of since it cannot be called on T\_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb\_ec\_setup\_exception is the only place where id\_cause is assigned from errinfo without checking if it is a throw\_data.

```

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
```

```
(errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```

```
...

Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>
---
eval.c | 4 ++++
1 file changed, 4 insertions(+)
```

Revision c96ef4ee - 07/18/2023 11:50 AM - U.Nakamura

merge revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe: [Backport #19593]

Ensure throw data is not set as cause

[Bug #19593]

rb_ec_setup_exception did not check if errinfo is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errinfo being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errinfo without checking if it is a throw_data.

```
...
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
(errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=
0, reverse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
...
```

```
Co-Authored-By: Jean Boussier <byroot@ruby-lang.org>
---
eval.c | 4 ++++
1 file changed, 4 insertions(+)
```

History

#1 - 04/12/2023 03:52 PM - peterzhu2118 (Peter Zhu)

- Backport changed from 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN to 3.0: REQUIRED, 3.1: REQUIRED, 3.2: REQUIRED

#2 - 04/13/2023 12:38 PM - peterzhu2118 (Peter Zhu)

- Status changed from Open to Closed

Applied in changeset [git\[02a7e12b80823919fb614ad3ea6241d5115d14fe\]](#).

Ensure throw data is not set as cause

[Bug [#19593](#)]

rb_ec_setup_exception did not check if errinfo is a throw_data. This can cause crashes in code since it is assumed that id_cause is an object.

We saw a crash in show_cause due to id_cause of errinfo being a throw_data. It crashes on rb_obj_is_kind_of since it cannot be called on T_IMEMO objects.

Unfortunately, we couldn't find a reproduction script, however we debugged the core dump and rb_ec_setup_exception is the only place where id_cause is assigned from errinfo without checking if it is a throw_data.

```
0x0000556c5708e6dd in sigsegv (sig=11, info=0x7f301befa3f0, ctx=0x7f301befa2c0) at signal.c:964
0x00007f301d046420 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
class_search_class_ancestor (c=139844586301760, cl=<optimized out>) at object.c:810
```

```
rb_obj_is_kind_of (obj=obj@entry=139839221734880, c=139844586301760) at object.c:861
0x0000556c56f2f00f in show_cause
    (errinfo=errinfo@entry=139838840645160, str=str@entry=139839221730520, opt=139839221730480, highlight=0, r
everse=reverse@entry=0, backtrace_limit=backtrace_limit@entry=-1, shown_causes=0x7ffe9d1a2d68) at ./include/ruby/internal/special_consts.h:175
```

Co-Authored-By: Jean Boussier byroot@ruby-lang.org

#3 - 07/17/2023 07:09 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 3.0: *REQUIRED*, 3.1: *REQUIRED*, 3.2: *REQUIRED* to 3.0: *REQUIRED*, 3.1: *REQUIRED*, 3.2: *DONE*

ruby_3_2 5fc9825ccf651664c547b1822c7f753464e27f06 merged revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe.

#4 - 07/18/2023 11:50 AM - usa (Usaku NAKAMURA)

- Backport changed from 3.0: *REQUIRED*, 3.1: *REQUIRED*, 3.2: *DONE* to 3.0: *REQUIRED*, 3.1: *DONE*, 3.2: *DONE*

ruby_3_1 c96ef4eee6b27796bb15ba161ef936998acbcf96 merged revision(s) 02a7e12b80823919fb614ad3ea6241d5115d14fe.