Ruby master - Bug #16019

please backport df317151a5b4e0c5a30fcc321a9dc6abad63f7ed

07/24/2019 11:37 PM - wanabe (_ wanabe)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.5: DONTNEED, 2.6: DONE

Description

TracePoint#enable can cause SEGV without df317151a5b4e0c5a30fcc321a9dc6abad63f7ed on ruby_2_6.

```
$ ((cd ../../; git checkout .); make install-nodoc -j4) >/dev/null 2>&1
$ ruby -v -e 'def foo; TracePoint.new(:b_return, &:disable).enable(target: method(:bar)); end;def
bar; 100.times{ foo; foo }; end; bar'
ruby 2.6.3p65 (2019-06-22 revision 67712) [x86_64-linux]
double free or corruption (fasttop)
Aborted (core dumped)
$
```

But it can't with df317151a5b4e0c5a30fcc321a9dc6abad63f7ed.

```
$ ((cd ../../; git checkout .; git show df317151a5b4e0c5a30fcc321a9dc6abad63f7ed vm_trace.c|patch
-p1); make install-nodoc -j4) >/dev/null 2>&1
$ ruby -v -e 'def foo; TracePoint.new(:b_return, &:disable).enable(target: method(:bar)); end;def
bar; 100.times{ foo; foo }; end; bar'
ruby 2.6.3p65 (2019-06-22 revision 67712) [x86_64-linux]
$
```

I think ruby_2_5 doesn't need the commit because TracePoint#enable accepts "target:" since 2.6.

Associated revisions

Revision fb8c28d3 - 08/18/2019 05:21 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) df317151a5b4e0c5a30fcc321a9dc6abad63f7ed: [Backport #16019]

```
    should not free local hook_list here.

    exec_hooks_postcheck() clean executed hook_list if it is needed.
    list_exec is freed if there are no events and this list is local
    event (connected to specific iseq). However, iseq keeps to point
    this local hook_list, freed list. To prevent this situation,
    do not free hook_list here even if it has no events.

    This issue is reported by @joker1007.
    https://twitter.com/joker1007/status/1153649170797830144
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67744 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 67744 - 08/18/2019 05:21 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) df317151a5b4e0c5a30fcc321a9dc6abad63f7ed: [Backport #16019]

```
should not free local hook_list here.

exec_hooks_postcheck() clean executed hook_list if it is needed.
list_exec is freed if there are no events and this list is local
event (connected to specific iseq). However, iseq keeps to point
this local hook_list, freed list. To prevent this situation,
do not free hook_list here even if it has no events.

This issue is reported by @joker1007.
https://twitter.com/joker1007/status/1153649170797830144
```

History

#1 - 07/29/2019 07:57 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.5: UNKNOWN, 2.6: UNKNOWN to 2.5: UNKNOWN, 2.6: REQUIRED

#2 - 08/18/2019 05:09 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.5: UNKNOWN, 2.6: REQUIRED to 2.5: DONTNEED, 2.6: REQUIRED

#3 - 08/18/2019 05:21 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.5: DONTNEED, 2.6: REQUIRED to 2.5: DONTNEED, 2.6: DONE

ruby_2_6 r67744 merged revision(s) df317151a5b4e0c5a30fcc321a9dc6abad63f7ed.