Ruby - Bug #20886

Crash due to double free on regex timeout after stack allocations

11/12/2024 05:06 AM - jhawthorn (John Hawthorn)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 3.3.6 (2024-11-05 revision 75015d4c1f) [x86_64-linux]	**Backport:**	3.1: DONTNEED, 3.2: DONTNEED, 3.3: DONE

Description

As of the change from #20650 (1057485) it's possible to crash on a double free due to stk_alloc AKA msa->stack_p being freed twice, once at the end of match_at and a second time in FREE_MATCH_ARG in the parent caller.

It's fairly, but not quite 100% reliable to reproduce, adjusting the timeout or number of spaces can help. I reduced this test case from a larger real-world regex, I believe the first part is important just to disable the match cache.

```
$ ruby -e 'Regexp.new("d()*+|a*a*bc", timeout: 0.2) === "b" + "a"*800'
double free or corruption (!prev)
```

https://github.com/ruby/ruby/pull/12030

Associated revisions

Revision 8409edc4971f34cf0d77c375909c5b8f7b1e058a - 11/12/2024 07:33 AM - jhawthorn (John Hawthorn)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

Revision 8409edc4971f34cf0d77c375909c5b8f7b1e058a - 11/12/2024 07:33 AM - jhawthorn (John Hawthorn)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

Revision 8409edc4 - 11/12/2024 07:33 AM - jhawthorn (John Hawthorn)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

Revision f4258aaed02ee7be761f2499b0b6243a8f37b7cb - 11/12/2024 05:04 PM - jhawthorn (John Hawthorn)

[Bug #20886] Avoid double-free in regex timeout after stack_double (#12063)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

Revision f4258aaed02ee7be761f2499b0b6243a8f37b7cb - 11/12/2024 05:04 PM - jhawthorn (John Hawthorn)

[Bug #20886] Avoid double-free in regex timeout after stack_double (#12063)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

Revision f4258aae - 11/12/2024 05:04 PM - jhawthorn (John Hawthorn)

[Bug #20886] Avoid double-free in regex timeout after stack_double (#12063)

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

History

#1 - 11/12/2024 07:41 AM - jhawthorn (John Hawthorn)

- Status changed from Open to Closed

Applied in changeset git|8409edc4971f34cf0d77c375909c5b8f7b1e058a.

Fix regex timeout double-free after stack_double

As of 10574857ce167869524b97ee862b610928f6272f, it's possible to crash
on a double free due to stk_alloc AKA msa->stack_p being freed
twice, once at the end of match_at and a second time in FREE_MATCH_ARG
in the parent caller.

Fixes [Bug #20886]

#2 - 11/12/2024 09:52 AM - jhawthorn (John Hawthorn)

I've opened a backport PR for Ruby 3.3. I don't believe other versions need a backport as the previous memory leak patches were not backported to the 3.2 branch and a quick test doesn't show the bug reproducing.

https://github.com/ruby/ruby/pull/12063

#3 - 01/15/2025 01:45 AM - k0kubun (Takashi Kokubun)

- Backport changed from 3.1: DONTNEED, 3.2: DONTNEED, 3.3: REQUIRED to 3.1: DONTNEED, 3.2: DONTNEED, 3.3: DONE

ruby_3_3 merged https://github.com/ruby/ruby/pull/12063. Thank you!