

Ruby - Bug #6144

regexec may allocate extra memory?

03/14/2012 07:44 PM - mame (Yusuke Endoh)

Status:	Closed	Backport:
Priority:	Normal	
Assignee:	naruse (Yui NARUSE)	
Target version:		
ruby -v:	ruby 2.0.0dev (2012-03-14 trunk 35017) [i686-linux]	

Description

naruse k-takata
naruse

regexec.c

```
alloc_addr = (char*)xalloca(sizeof(char*) * (ptr_num));\n\n#define STACK_INIT\n\nalloc_addr = (char*)xalloca(sizeof(char) * (ptr_num));\n\n\nalloc_addr = (char**)xalloca(sizeof(char*) * (ptr_num));\n\n\n\n\n\n\nCoverity Scan
```

--
Yusuke Endoh mame@tsg.ne.jp

History

#1 - 03/16/2012 12:21 AM - naruse (Yui NARUSE)

- Status changed from Open to Assigned

diff --git a/regexec.c b/regexec.c
index 2587cd9..9e31c71 100644
--- a/regexec.c
+++ b/regexec.c
@@ -446,16 +446,16 @@ onig_region_copy(OnigRegion* to, OnigRegion* from)\n\n#define STACK_INIT(alloc_addr, ptr_num, stack_num) do {\nif (msa->stack_p) {\n\n• alloc_addr = (char*)xalloca(sizeof(char*) * (ptr_num));\n\n• alloc_addr = (char*)xalloca(sizeof(OnigStackIndex*) * (ptr_num));\nstk_alloc = (OnigStackType*)(msa->stack_p);\nstk_base = stk_alloc;\nstk = stk_base;\nstk_end = stk_base + msa->stack_n;\n}\nelse {\n\n• alloc_addr = (char*)xalloca(sizeof(char*) * (ptr_num))\n

- alloc_addr = (char*)xalloca(sizeof(OnigStackIndex*) * (ptr_num) + sizeof(OnigStackType) * (stack_num));\
- stk_alloc = (OnigStackType*)(alloc_addr + sizeof(char*) * (ptr_num));\
- stk_alloc = (OnigStackType*)(alloc_addr + sizeof(OnigStackIndex*) * (ptr_num));
 stk_base = stk_alloc;
 stk = stk_base;
 stk_end = stk_base + (stack_num);\

#2 - 03/16/2012 12:36 AM - k_takata (Ken Takata)

```
alloc_addr OnigStackIndex* OnigStackIndex
OnigStackIndex intptr_t typedef xalloca
char* char*
```

```
alloc_addr = (OnigStackIndex*)xalloca(sizeof(OnigStackIndex) * (ptr_num));\
```

```
...
```

#3 - 03/16/2012 12:43 AM - k_takata (Ken Takata)

```
char* char*
stk_alloc char*
```

#4 - 03/21/2012 01:35 AM - k_takata (Ken Takata)

```
sizeof(char*) sizeof(OnigStackIndex)
```

<https://github.com/k-takata/Onigmo/tree/tmp/ruby-2.0.x>

#5 - 03/22/2012 09:21 AM - naruse (Yui NARUSE)

- Status changed from Assigned to Closed