Ruby master - Bug #4630

PROCDEBUG to non-zero values causes segmentation faults in check_env in trunk

04/29/2011 04:52 AM - ehuard (Elise Huard)

Status: Closed
Priority: Normal
Assignee: ko1 (Koichi Sasada)
Target version: 2.6
ruby -v: -
Backport: 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

Description
PROCDEBUG is meant to show debugging output from the vm.
However, when it's activated in vm.c
#define PROCDEBUG 1
The make process fails in segmentation faults.

I've narrowed it down to the following variables displayed in check_env: env->block.dfp[3] and env->block.dfp[4]
Commenting them out like so makes the segfaults disappear.

```c
static int
check_env(rb_env_t * const env)
{
    printf("---\n");
    printf("envptr: \%p\n", (void *)&env->block.dfp[0]);
    printf("orphan: \%p\n", (void *)&env->block.dfp[1]);
    printf("inheap: \%p\n", (void *)&env->block.dfp[2]);
    /* printf("envval: \%10p \", (void *)&env->block.dfp[3]);
       dp(env->block.dfp[3]);
    printf("penvv : \%10p \", (void *)&env->block.dfp[4]);
       dp(env->block.dfp[4]); */
    printf("lfp: \%10p\n", (void *)&env->block.lfp);
    printf("dfp: \%10p\n", (void *)&env->block.dfp);
    /* if (env->block.dfp[4]) {
       printf(">>>\n");
       check_env_value(env->block.dfp[4]);
       printf("<<<\n");
    } */
    return 1;
}
```

However, I'm not clued up enough on the inner workings of the VM to say why or how that should be fixed intelligently.

History

#1 - 06/10/2011 11:23 PM - ko1 (Koichi Sasada)
- ruby -v changed from 1.9.3dev to -

Hi,

(2011/04/29 4:52), Elise Huard wrote:

PROCDEBUG is meant to show debugging output from the vm.
However, when it's activated in vm.c
#define PROCDEBUG 1
The make process fails in segmentation faults.

Oops. I don't touch it on long time (because there is no bug which requires this debug option). So maybe this check_env() doesn't catch up Proc data structure.

--
// SASADA Koichi at atdot dot net

03/17/2022
#2 - 06/11/2011 04:33 PM - ko1 (Koichi Sasada)
- Category set to core
- Status changed from Open to Assigned
- Assignee set to ko1 (Koichi Sasada)
- Priority changed from Normal to 3

#3 - 06/26/2011 07:06 PM - nahi (Hiroshi Nakamura)
- Target version set to 2.0.0

#4 - 11/26/2012 09:21 AM - ko1 (Koichi Sasada)
- Target version changed from 2.0.0 to 2.6

#5 - 01/31/2017 09:12 AM - ko1 (Koichi Sasada)
- Status changed from Assigned to Closed
- Description updated

Now, we don't see this issue.