NEMU Bug报告

`numu` `bug`

南京大学匡亚明学院 刘志刚
学号：141242022

框架代码的一个bug

bug描述：

位置：nemu/src/monitor/debug/expr.c

```
1.  void init_regex() {
2.      int i;
3.      char error_msg[128];
4.      int ret;
5.
6.      for(i = 0; i < NR_REGEX; i ++) {
7.          ret = regcomp(&re[i], rules[i].regex, REG_EXTENDED);
8.          if(ret != 0) {
9.              regerror(ret, &re[i], error_msg, 128);
10.             Assert(ret != 0, "regex compilation failed: %s\n%s", error_
    msg, rules[i].regex);
11.         }
12.     }
13. }
```

应该将第10行的`Assert(ret!=0,...)`改为`Assert(ret==0,...)`，不然在遇到错误的正则串时，不会报错，会导致后续的regexec匹配失败，对于某些错误正则串会导致后续的regexec触发段错误。

发现过程：

我在帮一个同学调一个很闹鬼bug，我发现regexec会触发一个段错误，而且会导致之前的几个printf无法正常输出（abort之后，未刷新输出缓冲区）。我当时未注意到这是正则串的问题，我想即使匹配失败，也不应该触发一个段错误吧。我一度认为是regex库的bug。后来，我采取了对照未改动的框架代码，逐行添加的方式，最终发现是同学将"("的正则表达式写成了"(("，这就导致了这个错误。

在发现之后，我仍然以为这是regex库的bug，我今天自己另外拿regcomp来编译"("，后来发现regcomp正确地返回了非零值。后来，我再次检查框架代码中的init_regex()，才发现了这个问题的根源。修改之后，形如"("这样的错误正则串就不会编译通过，可以较早地定位问题。