1. 外发项目名称

cfgd

1. 执行平台

Linux NanoPi2 3.4.39-s5p4418 #4 SMP PREEMPT Mon Jun 11 11:26:13 CST 2018 armv7l GNU/Linux

1. 非常规版本发布原因及目的

致命 Bug尝试性修复

1. 详细说明
   1. bug产生自紫钺项目， 2020/12/18和2020/12/19 两次崩溃，崩溃信号均为SIGSEGV
   2. 现场core分析，两次堆栈一致，均表现为

#0 0xb6e0555c in vfprintf () from /lib/arm-linux-gnueabihf/libc.so.6

#1 0xb6e1f1fc in vsnprintf () from /lib/arm-linux-gnueabihf/libc.so.6

#2 0xb6f681b2 in pro\_append\_response (task=0xb7169bf8, format=0xb6f6c448 "%s\r\n") at pro/jesspro.c:66

#3 0xb6f6950e in pro\_execute\_task (task=0xb7169bf8) at pro/jesspro.c:506

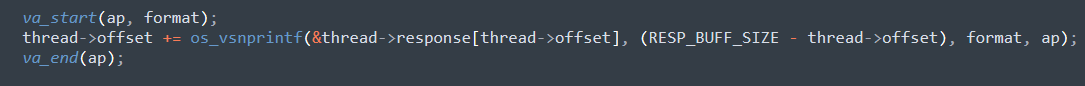
#4 0xb6f69816 in pro\_rotate\_task (thread=0xb5263008) at pro/jesspro.c:569

#5 0xb6f69896 in pro\_work\_routine (argv=0xb5263008) at pro/jesspro.c:585

#6 0xb6ed7f88 in start\_thread () from /lib/arm-linux-gnueabihf/libpthread.so.0

#7 0xb6e63ebc in ?? () from /lib/arm-linux-gnueabihf/libc.so.6

* 1. F2栈帧上所有局部变量无异常，F345栈帧上局部变量无异常
  2. 其余线程全部处于系统调用等待状态
  3. F2栈帧指向的vsnprintf的CRT调用方式正常，参数和缓冲区正常
  4. 原bug代码片段

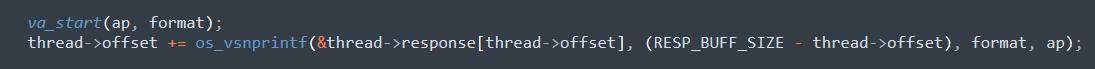


* 1. 问题辅助文档片段

The functions vprintf(), vfprintf(), vsprintf(), vsnprintf() are equivalent to the functions printf(), fprintf(), sprintf(), snprintf(), respectively, except that they are called with a va\_list

instead of a variable number of arguments. These functions do not call the va\_end macro. Because they invoke the va\_arg macro, **the value of ap is undefined after the call.**

* 1. 修改后的代码片段



1. 简略升级版本静态代码检测结果

Checking args.c ...

Checking args.c: GLOBAL\_ARGS\_H...

1/20 files checked 1% done

Checking cJSON.c ...

Checking cJSON.c: CJSON\_API\_VISIBILITY;\_\_GNUC\_\_;\_\_SUNPRO\_C;\_\_SUNPRO\_CC...

Checking cJSON.c: CJSON\_EXPORT\_SYMBOLS;CJSON\_HIDE\_SYMBOLS;CJSON\_IMPORT\_SYMBOLS...

Checking cJSON.c: CJSON\_HIDE\_SYMBOLS...

Checking cJSON.c: CJSON\_IMPORT\_SYMBOLS...

Checking cJSON.c: ENABLE\_LOCALES...

Checking cJSON.c: WIN32;WIN64;\_MSC\_VER;\_WIN32;\_\_WINDOWS\_\_...

Checking cJSON.c: \_CRT\_SECURE\_NO\_DEPRECATE;\_MSC\_VER...

Checking cJSON.c: \_MSC\_VER...

Checking cJSON.c: \_\_GNUC\_\_...

Checking cJSON.c: \_\_GNUC\_\_;\_\_clang\_\_...

Checking cJSON.c: false...

2/20 files checked 29% done

Checking easyjess/easybin.c ...

3/20 files checked 32% done

Checking easyjess/easyjess.c ...

Checking easyjess/easyjess.c: NSPTST\_HEAD...

Checking easyjess/easyjess.c: NSPTST\_HEAD;\_WIN32...

Checking easyjess/easyjess.c: \_WIN32...

4/20 files checked 38% done

Checking easyjess/easyjess2.c ...

Checking easyjess/easyjess2.c: \_WIN32...

5/20 files checked 41% done

Checking easyjess/subscribe.c ...

Checking easyjess/subscribe.c: EASYJESS\_H...

Checking easyjess/subscribe.c: EASYJESS\_H;\_WIN32...

Checking easyjess/subscribe.c: EASYJESS\_H;\_WIN32;posix\_\_atomic\_get...

Checking easyjess/subscribe.c: EASYJESS\_H;\_WIN32;posix\_\_atomic\_set...

Checking easyjess/subscribe.c: \_WIN32...

6/20 files checked 44% done

Checking fs/checkpoint.c ...

Checking fs/checkpoint.c: JESSFS\_H...

7/20 files checked 46% done

Checking fs/inner.c ...

Checking fs/inner.c: JESSFS\_H...

8/20 files checked 47% done

Checking fs/jessfs.c ...

Checking fs/jessfs.c: JESSFS\_H...

9/20 files checked 54% done

Checking fs/proc.c ...

Checking fs/proc.c: JESSFS\_H...

Checking fs/proc.c: \_WIN32...

10/20 files checked 56% done

Checking jess.c ...

Checking jess.c: GLOBAL\_ARGS\_H...

Checking jess.c: NETOBJECT\_H...

11/20 files checked 57% done

Checking jessnet.c ...

Checking jessnet.c: NETOBJECT\_H...

Checking jessnet.c: NSPTST\_HEAD...

Checking jessnet.c: NSPTST\_HEAD;\_WIN32...

12/20 files checked 62% done

Checking ldr/jessldr.c ...

Checking ldr/jessldr.c: JSONIFY\_LOADED\_H...

13/20 files checked 68% done

Checking os/jessos.c ...

Checking os/jessos.c: JESSOS\_H...

Checking os/jessos.c: JESSOS\_H;\_WIN32...

Checking os/jessos.c: \_WIN32...

14/20 files checked 72% done

Checking pro/binary.c ...

Checking pro/binary.c: JESS\_PROTO\_H...

15/20 files checked 72% done

Checking pro/jesspro.c ...

Checking pro/jesspro.c: JESS\_PROTO\_H...

16/20 files checked 80% done

Checking pro/manage.c ...

Checking pro/manage.c: JESS\_PROTO\_H...

17/20 files checked 81% done

Checking pro/variable.c ...

Checking pro/variable.c: JESS\_PROTO\_H...

18/20 files checked 84% done

Checking runtime/request.c ...

Checking runtime/request.c: JESSRT\_REQUESTER\_H...

Checking runtime/request.c: JSONIFY\_ESCAPE\_H...

Checking runtime/request.c: JSONIFY\_ESCAPE\_H;\_UNIT\_TEST...

Checking runtime/request.c: JSONIFY\_ESCAPE\_H;\_UNIT\_TEST;\_WIN32...

Checking runtime/request.c: JSONIFY\_ESCAPE\_H;\_WIN32...

Checking runtime/request.c: \_UNIT\_TEST...

19/20 files checked 87% done

Checking runtime/runtime.c ...

Checking runtime/runtime.c: JESSRT\_REQUESTER\_H...

Checking runtime/runtime.c: JSONIFY\_ESCAPE\_H...

Checking runtime/runtime.c: JSONIFY\_ESCAPE\_H;\_UNIT\_TEST...

Checking runtime/runtime.c: JSONIFY\_ESCAPE\_H;\_UNIT\_TEST;\_WIN32...

Checking runtime/runtime.c: JSONIFY\_ESCAPE\_H;\_WIN32...

Checking runtime/runtime.c: \_WIN32...

20/20 files checked 100% done

1. 内测用例涵盖

Read x20

Write x20

Scope x5

File x5

Contain x10

1. 执行程序MD5

5c6616e3f8e7faf2679bc1571470382c jess.arm32

1. Git Tag

1.5.2