Problem 2

1. Project Name

Openjpeg

2. Source Code Version

Version 2.1.2

https://github.com/uclouvain/openjpeg/releases/tag/v2.1.2

3. PoC Downloadable from Internet?

Yes

4. CVE ID

CVE-2016-10506

5. Details Procedures that trigger the crash

a. How the project program is compiled.

The program is compiled using the installation method described by the GitHub source:

1. Go to the directory of the project program and type:
2. mkdir
3. cd build
4. cmake .. –DCMAKE_BUILD_TYPE=Release
5. make
6. `sudo apt-get install liblcms2-dev libtiff-dev libpng-dev libz-dev`

b. The exact running arguments

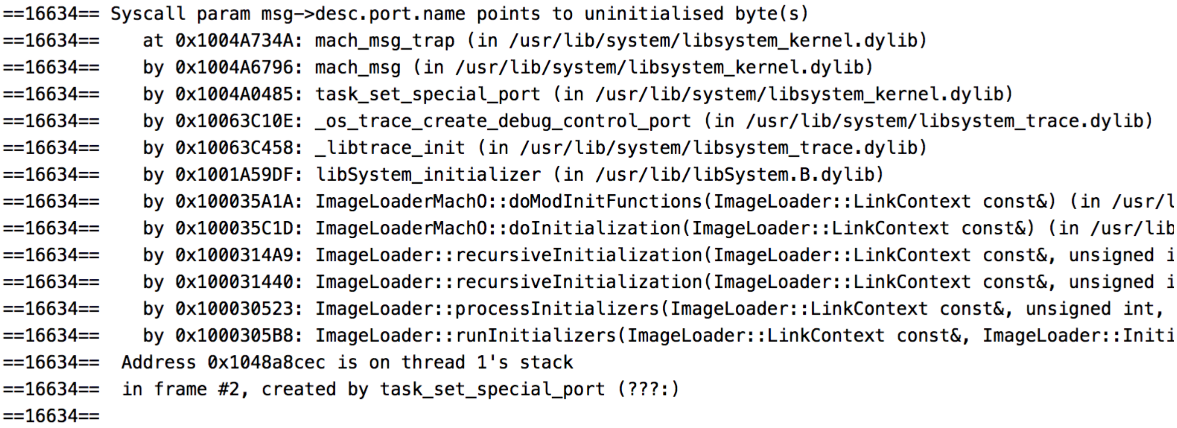
1. Go to project_program/build/bin,

2. Add in the input file “poc5.j2k”

3. Type: “valgrind opj_decompress -i in/poc5.j2k -o out/poc5.png”

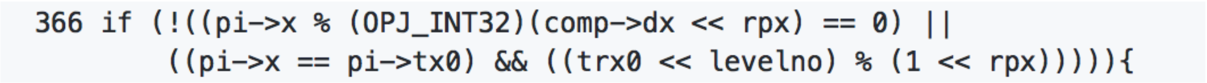
Crash Description

The crash found occurs due to a jump based on an uninitialized variable:



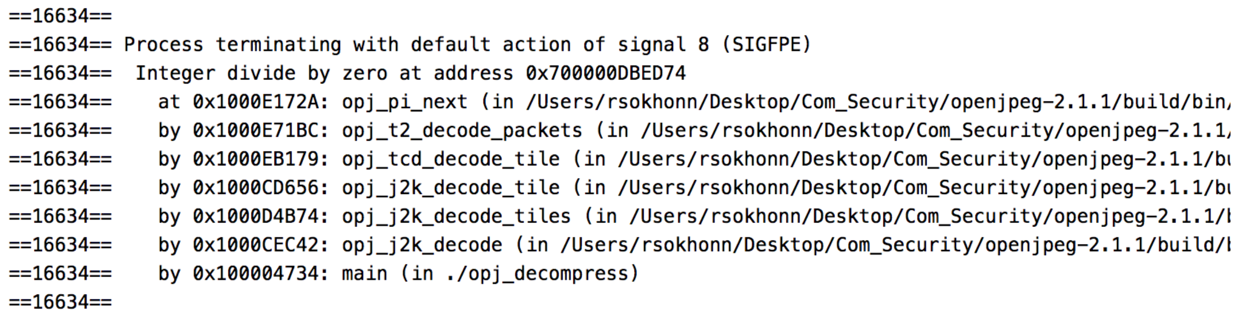
```
==16634== Syscall param msg->desc.port.name points to uninitialised byte(s)
==16634==    at 0x1004A734A: mach_msg_trap (in /usr/lib/system/libsystem_kernel.dylib)
==16634==    by 0x1004A6796: mach_msg (in /usr/lib/system/libsystem_kernel.dylib)
==16634==    by 0x1004A0485: task_set_special_port (in /usr/lib/system/libsystem_kernel.dylib)
==16634==    by 0x10063C10E: _os_trace_create_debug_control_port (in /usr/lib/system/libsystem_trace.dylib)
==16634==    by 0x10063C458: _libtrace_init (in /usr/lib/system/libsystem_trace.dylib)
==16634==    by 0x1001A59DF: libSystem_initializer (in /usr/lib/libSystem.B.dylib)
==16634==    by 0x100035A1A: ImageLoaderMachO::doModInitFunctions(ImageLoader::LinkContext const&) (in /usr/l
==16634==    by 0x100035C1D: ImageLoaderMachO::doInitialization(ImageLoader::LinkContext const&) (in /usr/lib
==16634==    by 0x1000314A9: ImageLoader::recursiveInitialization(ImageLoader::LinkContext const&, unsigned i
==16634==    by 0x100031440: ImageLoader::recursiveInitialization(ImageLoader::LinkContext const&, unsigned i
==16634==    by 0x100030523: ImageLoader::processInitializers(ImageLoader::LinkContext const&, unsigned int,
==16634==    by 0x1000305B8: ImageLoader::runInitializers(ImageLoader::LinkContext const&, ImageLoader::Initi
==16634==  Address 0x1048a8cec is on thread 1's stack
==16634==  in frame #2, created by task_set_special_port (???:)
==16634==
```

The vulnerability is a “division-by-zero” vulnerability in the function, “opj_pi_next_rpcl”, of pi.c.The error occurs at line 366:



```
366 if (!((pi->x % (OPJ_INT32)(comp->dx << rpx) == 0) ||
        ((pi->x == pi->tx0) && ((trx0 << levelno) % (1 << rpx))))){
```

The crash is caused by an integer division at the root address 0x1000E172A when the address 0x100004734 is called:

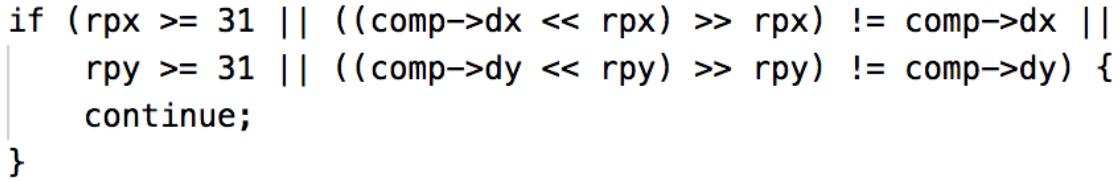


```
==16634==
==16634== Process terminating with default action of signal 8 (SIGFPE)
==16634==  Integer divide by zero at address 0x700000DBED74
==16634==    at 0x1000E172A: opj_pi_next (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/build/bin/
==16634==    by 0x1000E71BC: opj_t2_decode_packets (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/
==16634==    by 0x1000EB179: opj_tcd_decode_tile (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/bu
==16634==    by 0x1000CD656: opj_j2k_decode_tile (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/bu
==16634==    by 0x1000D4B74: opj_j2k_decode_tiles (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/b
==16634==    by 0x1000CEC42: opj_j2k_decode (in /Users/rsokhonn/Desktop/Com_Security/openjpeg-2.1.1/build/b
==16634==    by 0x100004734: main (in ./opj_decompress)
==16634==
```

This vulnerability allows remote attackers to cause a denial of service (application crash) via crafted j2k files.

Brief explanation about bug fixed.

The bug can be fixed by putting an undefined behaviour on shift to avoid division by zero.



```
if (rpx >= 31 || ((comp->dx << rpx) >> rpx) != comp->dx ||
    rpy >= 31 || ((comp->dy << rpy) >> rpy) != comp->dy) {
    continue;
}
```