Problem 2

1. Project Name

ImageMagick

2. Source Code Version

Version 7.0.6.0
https://github.com/ImageMagick/ImageMagick/releases/tag/7.0.6-0

3. PoC Downloadable from Internet?

Yes

4. CVE ID

CVE-2017-15281

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. make
3. sudo make install
4. magick --version

b. The exact running arguments

1. Add in the input file “poc2”
2. Type: “valgrind convert in/poc2 out/poc2”

Crash Description

The crash occurs due to a jump based on an uninitialized variable in a malformed input file:

```
==9218== Syscall param msg->desc.port.name points to uninitialised byte(s)
==9218==    at 0x10084534A: mach_msg_trap (in /usr/lib/system/libsystem_kernel.dylib)
==9218==    by 0x100844796: mach_msg (in /usr/lib/system/libsystem_kernel.dylib)
==9218==    by 0x10083E485: task_set_special_port (in /usr/lib/system/libsystem_kernel.dylib)
==9218==    by 0x1009DA10E: _os_trace_create_debug_control_port (in /usr/lib/system/libsystem_trace.dylib)
==9218==    by 0x1009DA458: _libtrace_init (in /usr/lib/system/libsystem_trace.dylib)
==9218==    by 0x1005439DF: libSystem_initializer (in /usr/lib/libSystem.B.dylib)
==9218==    by 0x100018A1A: ImageLoaderMachO::doModInitFunctions(ImageLoader::LinkContext const&) (in /usr/lib/dyld)
==9218==    by 0x100018C1D: ImageLoaderMachO::doInitialization(ImageLoader::LinkContext const&) (in /usr/lib/dyld)
==9218==    by 0x1000144A9: ImageLoader::recursiveInitialization(ImageLoader::LinkContext const&, unsigned int, char const*,
==9218==    by 0x100014440: ImageLoader::recursiveInitialization(ImageLoader::LinkContext const&, unsigned int, char const*,
==9218==    by 0x100013523: ImageLoader::processInitializers(ImageLoader::LinkContext const&, unsigned int, ImageLoader::Ini
==9218==    by 0x1000135B8: ImageLoader::runInitializers(ImageLoader::LinkContext const&, ImageLoader::InitializerTimingList
==9218==  Address 0x10488bd7c is on thread 1's stack
==9218==  in frame #2, created by task_set_special_port (???:)
```

The picture below shows the memory of the jump where the error occurred at 0x100000D90 caused by the root address 0x1001A5308:

```
==9218== Conditional jump or move depends on uninitialised value(s)
==9218==    at 0x1001A5308: ExportQuantumPixels (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x100284DA0: WritePSDChannel (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x1002848A9: WritePSDChannels (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x100282C58: WritePSDImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x1000DE2A4: WriteImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x1000DE788: WriteImages (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9218==    by 0x1004389E3: ConvertImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9218==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9218==    by 0x100000D90: main (in /usr/local/bin/convert)
```

Brief explanation about bug fixed.

The bug is fixed by having an exception to check for corrupted or malformed image files.