Project Name

Proof of Crash 1: OpenJPEG Heap-Based Buffer Overflow

Source Code Version

OpenJPEG 2.2.0

Github Link: https://github.com/uclouvain/openjpeg/releases/tag/v2.2.0

Commit ID: `3d7cde5fc9fbc5618d02160900d32e02ed12a00e (3d7cde5)`

PoC downloadable from the internet

CVE ID

CVE-2017-14039

Link: http://www.cvedetails.com/cve/CVE-2017-14039/

The detailed procedures that trigger the crash

How the project programs are compiled:

CMake

Download CMake: https://cmake.org/files/v3.9/cmake-3.9.6.tar.gz

Run the **`bootstrap`** script in the source directory of CMake.

Once this has finished successfully, run **`make`** and then **`make install`**.

In summary:

```
./bootstrap
make
make install
```

OpenJPEG 2.2.0

To build the library, type from source tree directory:

```
mkdir build
cd build
cmake .. -DCMAKE_BUILD_TYPE=Release
make
```

Binaries are then located in the `bin` directory.

To install the library, type with root privileges:

```
make install
make clean
```

The exact running arguments:

```
opj_compress -r 20,10,1 -jpip -EPH -SOP -cinema2K 24 -n 1 -i $FILE -o null.j2k
```

$FILE is the file name and location. In this case, replace it to **`input.tif`**.

A description about the crashes

Program location of crash: the **opj_t2_encode_packet** function in **lib/openjp2/t2.c**

Description: A heap-based buffer overflow in the function causes an out-of-bounds write.

A brief explanation about the bug fixes

Bug fixes snippet from the following commit:
https://github.com/uclouvain/openjpeg/commit/c535531f03369623b9b833ef41952c62257b507e

In the file `src/lib/openjp2/j2k.c`:

```
if (p_total_data_size < 4) {
    opj_event_msg(p_manager, EVT_ERROR,
        "Not enough bytes in output buffer to write SOD marker\n");
    return OPJ_FALSE;
}
```

And in the file `src/lib/openjp2/t2.c`:

```
if (length < 6) {
    if (p_t2_mode == FINAL_PASS) {
               opj_event_msg(p_manager, EVT_ERROR,
               "opj_t2_encode_packet(): only %u bytes remaining in "
               "output buffer. %u needed.\n",
               length, 6);
       }
       return OPJ_FALSE;
}
```

```
if (length < 2) {
    if (p_t2_mode == FINAL_PASS) {
        opj_event_msg(p_manager, EVT_ERROR,
               "opj_t2_encode_packet(): only %u bytes remaining in "
               "output buffer. %u needed.\n",
               length, 2);
      }
    return OPJ_FALSE;
}
```

To prevent buffer overflow, the bug fixes add a check if the length of the buffer exceeds the limit (in this case: 4, 6, and 2 respectively), it returns an error message.