Project Name
OpenJPEG

Source Code Version:
2.2.0
Poc downloadable

CVE ID
CVE-2017-14164

Program Crash Procedure

1. Download OpenJPEG v2.2.0 for linux from https://github.com/uclouvain/openjpeg/releases/tag/v2.2.0
2. Extract .tar.gz file as downloaded above
3. on terminal, enter extracted openjpeg directory
4. mkdir -v build
5. cd build
6. cmake -DCMAKE_BUILD_TYPE=Release -DCMAKE_INSTALL_PREFIX=/usr ..
7. make
8. sudo make install
9. pushd ../doc &&
10. for man in man/man?/* ; do
    install -v -D -m 644 $man /usr/share/$man
    done
    popd

11. Input in terminal:
    opj_compress -r 20,10,1 -jpip -EPH -SOP -cinema2K 24 -n 1 -i test.tif -o null.j2k
    (test.tif can be found in the folder)

Crash Details
Program Location of Root Cause
In the file src/lib/openjp2/j2k.c

Program Location of Crash
opj_j2k_write_sot()

OpenJPEG is prone to a remote heap-based buffer-overflow vulnerability because it fails to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer.

An attacker can exploit this issue to crash the affected application, resulting in denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed. Overwriting heap memory content with values that an attacker has crafted allows the attacker to execute arbitrary code in the affected computer.

In the test case provided above, a .tiff file that exceeds the allocated input memory buffer is fed to OpenJPEG to trigger this crash. As suggested in the error output, OpenJPEG attempts to overwrite the heap when this input file is fed to it. This vulnerability was fixed in the next patch of OpenJPEG.

Bug Fixes
Commit that fixes the bug
https://github.com/uclouvain/openjpeg/commit/dcac91b8c72f743bda7dbfa9032356bc8110098a

This fix introduces a new variable, p_total_data_size which contains the size of buffer currently available for file storage. This variable is used in opj_j2k_write_sot() to perform boundary-checks to prevent heap-based overflow. This fix will prompt an error and disallow request for file storage, which will stop OpenJPEG before doing any harm to the memory.

Summary
Heap-based buffer-overflow vulnerability is very common and can potentially be used by attackers to overwrite memory and pointer contents. Therefore, boundary checks should always be conducted before a program processes data from a user.

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

https://github.com/uclouvain/openjpeg/commit/dcac91b8c72f743bda7dbfa9032356bc8110098a

http://www.cvedetails.com/cve/CVE-2017-14164/

https://blogs.gentoo.org/ago/2017/09/06/heap-based-buffer-overflow-in-opj_write_bytes_le-cio-c-incomplete-fix-for-cve-2017-14152/