Vorbis - oggenc

Source Code Version

Affected Version : 1.4.0
Source Code URL : https://github.com/xiph/vorbis-tools

Managed using GitHub Git version control.

Whether the PoC is downloadable from Internet

Yes but it cannot be used directly
https://trac.xiph.org/ticket/2137#no1

CVE ID

CVE-2014-9638
http://www.cvedetails.com/cve/CVE-2014-9638/

The detailed procedures that trigger the crash

How the project programs are compiled :

1. Download the source code using wget http://downloads.xiph.org/releases/vorbis/vorbis-tools-1.4.0.tar.gz
2. Go to the downloaded directory
3. Make a build folder using mkdir build
4. Go into the *build* directory
5. Invoke the configure script, points compiler to afl compiler and enable the use of Address Sanitizer. This can be done by this line AFL_USE_ASAN=1 ./../configure CC=afl-gcc CXX=afl-g++ LD=afl-gcc--disable-shared
6. Compile/Make the code by using AFL_USE_ASAN=1 make

Note: AFL_USE_ASAN=1 is to enable the use of Address Sanitizer

The exact running arguments

1. Go to the *oggdec* directory after compiling the code

2. Recreate the crash by running the following code `./oggdec $FILE` where the *$FILE* is the input provided

Description about the crashes (program locations of crash, program locations of the root cause)

Program crashed due to channel = 0 and using channel as the denominator at line 137 under oggdec/oggdec.c.

Explanation about the bug fixes

Check if the channel is 0 before dividing. Terminate the program if channel is 0.