LHA

Source Code Version

Affected Version : 1.14i-ac20050924p1
Source Code URL : https://github.com/jca02266/lha

Managed using GitHub Git version control.

Whether the PoC is downloadable from Internet

No

CVE ID

No CVE ID.
Crash is founded by the group.

The detailed procedures that trigger the crash

How the project programs are compiled :

1. Download the source code using `git clone https://github.com/jca02266/lha`
2. Go to the downloaded directory
3. Generate the ‘configuration’ script by using GNU autoconf tools. Run the following in sequence:
    a. aclocal
    b. autoheader
    c. automake -a
    d. autoconf
4. Make a build folder using `mkdir build`
5. Go into the *build* directory
6. 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`
7. 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 *src* directory after compiling the code
2. Recreate the crash by running the following code `./lha -x $FILE -w /tmp` where the *$FILE* is the input provided

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

Vfprintf is not a thread safe program. When LHA is trying to print out the error. The malformed argument caused the heap-based over read read (Segmentation Fault), when ASAN is disabled, it will show segmentation fault.

Explanation about the bug fixes

vprintf() is used at line 725 & 479 under src/lharc.c. This is not a thread safe function.
By changing from:

```
vfprintf(stderr, fmt, v);
```

to:

```
vfprintf_s(stderr, fmt, v);
```

will prevent the heap-based over read issue.