Starred by 2 users

Owner:	----
CC:	r...@sanger.ac.uk a...@sanger.ac.uk v...@sanger.ac.uk j...@sanger.ac.uk
Status:	Verified *(Closed)*
Components:	----
Modified:	Aug 15, 2020
Type:	Bug-Security

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Stability-UndefinedBehaviorSanitizer
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-htslib
Reported-2020-07-12
Disclosure-2020-10-12

Issue 24097: htslib:hts_open_fuzzer: Crash in vcf_parse_format

Reported by ClusterFuzz-External on Sun, Jul 12, 2020, 7:33 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5755637137670144

Project: htslib
Fuzzing Engine: libFuzzer
Fuzz Target: hts_open_fuzzer
Job Type: libfuzzer_ubsan_htslib
Platform Id: linux

Crash Type: UNKNOWN WRITE
Crash Address: 0x7fe46ff161c0
Crash State:
  vcf_parse_format
  vcf_parse
  vcf_read

Sanitizer: undefined (UBSAN)

Recommended Security Severity: High

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_htslib&revision=202007120253

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5755637137670144

Issue filed automatically.

See https://google.github.io/oss-fuzz/advanced-topics/reproducing for instructions to reproduce this bug locally.
When you fix this bug, please
  * mention the fix revision(s).
  * state whether the bug was a short-lived regression or an old bug in any stable releases.
  * add any other useful information.
This information can help downstream consumers.

If you need to contact the OSS-Fuzz team with a question, concern, or any other feedback, please file an issue at https://github.com/google/oss-fuzz/issues. Comments on individual Monorail issues are not monitored.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse
without an upstream patch, then the bug report will automatically
become visible to the public.

Comment 1 by sheriffbot on Tue, Jul 14, 2020, 4:15 PM EDT Project Member

Labels: Disclosure-2020-10-12

Comment 2 by ClusterFuzz-External on Thu, Jul 16, 2020, 10:54 AM EDT Project Member

Status: Verified (was: New)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5755637137670144 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_htslib&range=202007150254:202007160254

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 3 by sheriffbot on Sat, Aug 15, 2020, 4:03 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot