Starred by 1 user

Owner:	----
CC:	p.ant...@catenacyber.fr luca....@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	May 18, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Deadline-Exceeded
Engine-libfuzzer
OS-Linux
Fuzz-Blocker
Security_Severity-High
Proj-ndpi
Reported-2021-02-06
Disclosure-2021-05-07

Issue 30393: ndpi:fuzz_process_packet: Stack-buffer-overflow in processClientServerHello

Reported by ClusterFuzz-External on Sat, Feb 6, 2021, 11:50 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4831031280664576

Project: ndpi
Fuzzing Engine: libFuzzer
Fuzz Target: fuzz_process_packet
Job Type: libfuzzer_asan_ndpi
Platform Id: linux

Crash Type: Stack-buffer-overflow WRITE 6
Crash Address: 0x7ffe7ac81ff3
Crash State:
  processClientServerHello
  processTLSBlock
  ndpi_search_tls_tcp

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_ndpi&range=202007270341:202007280346

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4831031280664576

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 ClusterFuzz-External on Sat, Feb 6, 2021, 12:57 PM EST Project Member

Labels: Fuzz-Blocker

This crash occurs very frequently on linux platform and is likely preventing the fuzzer fuzz_process_packet from making much progress. Fixing this will allow more bugs to be found.

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

Comment 2 by sheriffbot on Sat, Feb 6, 2021, 3:02 PM EST Project Member

Labels: Disclosure-2021-05-07

Comment 3 by sheriffbot on Fri, Apr 30, 2021, 2:47 PM EDT Project Member

Labels: Deadline-Approaching

This bug is approaching its deadline for being fixed, and will be automatically derestricted within 7 days. If a fix is planned within 2 weeks after the deadline has passed, a grace extension can be granted.

- Your friendly Sheriffbot

Comment 4 by sheriffbot on Fri, May 7, 2021, 2:52 PM EDT Project Member

Labels: -restrict-view-commit -deadline-approaching Deadline-Exceeded

This bug has exceeded our disclosure deadline. It has been opened to the public.

- Your friendly Sheriffbot

Comment 5 by ClusterFuzz-External on Tue, May 18, 2021, 10:52 AM EDT Project Member

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

ClusterFuzz testcase 4831031280664576 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_ndpi&range=202105170629:202105180628

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