☆ Starred by 2 users

Owner:	----
CC:	p.ant...@catenacyber.fr luca....@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Jun 12, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Stability-AFL
OS-Linux
Engine-afl
Security_Severity-Medium
Proj-ndpi
Reported-2020-04-18
Disclosure-2020-07-17

Issue 21780: ndpi:fuzz_process_packet: Heap-buffer-overflow in ndpi_search_oracle

Reported by ClusterFuzz-External on Sat, Apr 18, 2020, 12:07 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5090959332474880

Project: ndpi
Fuzzing Engine: afl
Fuzz Target: fuzz_process_packet
Job Type: afl_asan_ndpi
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 1
Crash Address: 0x60a0000fbad1
Crash State:
  ndpi_search_oracle
  check_ndpi_tcp_flow_func
  ndpi_detection_process_packet

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Crash Revision: https://oss-fuzz.com/revisions?job=afl_asan_ndpi&revision=202003230257

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5090959332474880

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 Sat, Apr 18, 2020, 4:12 PM EDT Project Member

Labels: Disclosure-2020-07-17

Comment 2 by ClusterFuzz-External on Wed, May 13, 2020, 12:46 PM EDT Project Member

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

ClusterFuzz testcase 5090959332474880 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_ndpi&range=202005120255:202005130255

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

Comment 3 by sheriffbot on Fri, Jun 12, 2020, 4:01 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