Starred by 1 user

Owner:	----
CC:	wpp...@amazon.com edsi...@gmail.com da...@adalogics.com
Status:	Verified *(Closed)*
Components:	----
Modified:	May 7, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Security_Severity-High
Engine-honggfuzz
Proj-fluent-bit
Disclosure-2021-07-26
Reported-2021-04-27

Issue 33750: fluent-bit:flb-it-fuzz-parser_fuzzer_OSSFUZZ: Heap-double-free in flb_free

Reported by ClusterFuzz-External on Tue, Apr 27, 2021, 2:27 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5216297967288320

Project: fluent-bit
Fuzzing Engine: honggfuzz
Fuzz Target: flb-it-fuzz-parser_fuzzer_OSSFUZZ
Job Type: honggfuzz_asan_fluent-bit
Platform Id: linux

Crash Type: Heap-double-free
Crash Address: 0x625000002900
Crash State:
  flb_free
  flb_parser_json_do
  flb_parser_do

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=honggfuzz_asan_fluent-bit&range=202101270627:202101280616

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5216297967288320

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, Apr 27, 2021, 3:09 PM EDT Project Member

Labels: Disclosure-2021-07-26

Comment 2 by ClusterFuzz-External on Fri, May 7, 2021, 10:21 AM EDT Project Member

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

ClusterFuzz testcase 5216297967288320 is verified as fixed in https://oss-fuzz.com/revisions?job=honggfuzz_asan_fluent-bit&range=202105060607:202105070621

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

Comment 3 by sheriffbot on Fri, May 7, 2021, 2:57 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed. It has been opened to the public.

- Your friendly Sheriffbot