Starred by 2 users

Owner: ----

CC: wpp...@amazon.com
edsi...@gmail.com
da...@adalogics.com

Status: Verified *(Closed)*

Components: ----

Modified: Dec 8, 2020

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Fuzz-Blocker
Security_Severity-High
Engine-honggfuzz
Proj-fluent-bit
Reported-2020-11-06
Disclosure-2021-02-04

Issue 27261: fluent-bit:flb-it-fuzz-utils_fuzzer_OSSFUZZ: Heap-buffer-overflow in flb_gzip_compress

Reported by ClusterFuzz-External on Fri, Nov 6, 2020, 5:24 PM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4662513180082176

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

Crash Type: Heap-buffer-overflow WRITE 1
Crash Address: 0x631000088f1e
Crash State:
  flb_gzip_compress
  utils_fuzzer.c

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=honggfuzz_asan_fluent-bit&range=202010220618:202010230607

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4662513180082176

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 Fri, Nov 6, 2020, 5:25 PM EST Project Member

Labels: Fuzz-Blocker

This crash occurs very frequently on linux platform and is likely preventing the fuzzer flb-it-fuzz-utils_fuzzer_OSSFUZZ 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, Nov 7, 2020, 3:05 PM EST Project Member

Labels: Disclosure-2021-02-04

Comment 3 by ClusterFuzz-External on Sun, Nov 8, 2020, 10:29 AM EST Project Member

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

ClusterFuzz testcase 4662513180082176 is verified as fixed in https://oss-fuzz.com/revisions?job=honggfuzz_asan_fluent-bit&range=202011070625:202011080619

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

Comment 4 by sheriffbot on Tue, Dec 8, 2020, 2:55 PM EST Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot