Starred by 1 user

Owner: ----

CC: yak...@code-intelligence.com
wag...@code-intelligence.com
patri...@code-intelligence.com
glend...@code-intelligence.com

Status: Verified *(Closed)*

Components: ----

Modified: May 17, 2022

Type: Bug-Security

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-Low
Proj-snakeyaml

Issue 47027: snakeyaml:YamlFuzzer: Uncaught exception in org.yaml.snakeyaml.constructor.BaseConstructor.constructObject

Reported by ClusterFuzz-External on Tue, Apr 26, 2022, 4:26 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5427149240139776

Project: snakeyaml
Fuzzing Engine: libFuzzer
Fuzz Target: YamlFuzzer
Job Type: libfuzzer_asan_snakeyaml
Platform Id: linux

Crash Type: Uncaught exception
Crash Address:
Crash State:
  org.yaml.snakeyaml.constructor.BaseConstructor.constructObject
  org.yaml.snakeyaml.constructor.BaseConstructor.constructSequenceStep2
  org.yaml.snakeyaml.constructor.BaseConstructor.constructSequence

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_asan_snakeyaml&revision=202204260602

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5427149240139776

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 26, 2022, 2:55 PM EDT Project Member

Labels: Disclosure-2022-07-25

Comment 2 by ClusterFuzz-External on Sun, May 1, 2022, 12:55 PM EDT Project Member

Status: Verified (was: New)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5427149240139776 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_snakeyaml&range=202204290605:202205010601

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

Comment 3 by sheriffbot on Mon, May 2, 2022, 2:45 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot

Comment 4 by ClusterFuzz-External on Tue, May 17, 2022, 4:06 AM EDT Project Member

Labels: -Reported-2022-04-26 -Disclosure-2022-07-25