Starred by 1 user

Owner: ----

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

Status: Verified *(Closed)*

Components: ----

Modified: Aug 22, 2022

Type: Bug-Security

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

Issue 50428: xstream:XmlFuzzer: Security exception in com.ctc.wstx.dtd.FullDTDReader.readContentSpec

Reported by ClusterFuzz-External on Thu, Aug 18, 2022, 9:48 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=6365800201584640

Project: xstream
Fuzzing Engine: libFuzzer
Fuzz Target: XmlFuzzer
Job Type: libfuzzer_asan_xstream
Platform Id: linux

Crash Type: Security exception
Crash Address:
Crash State:
  com.ctc.wstx.dtd.FullDTDReader.readContentSpec
  java.base/sun.nio.cs.CESU_8.updatePositions
  java.base/sun.nio.cs.CESU_8$Encoder.encodeArrayLoop

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_xstream&range=202208170608:202208180608

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=6365800201584640

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.

Comment 1 by ClusterFuzz-External on Mon, Aug 22, 2022, 10:50 AM EDT Project Member

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

ClusterFuzz testcase 6365800201584640 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_xstream&range=202208210610:202208220611

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

Comment 2 by sheriffbot on Mon, Aug 22, 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