

oss-fuzz

oss-fuzz

New issue

Open issues



Search oss-fuzz issues...



Sign in

☆ 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:

Sep 7, 2022

Type:

[Bug-Security](#)

ClusterFuzz

Reproducible

ClusterFuzz-Verified

Engine-libfuzzer

OS-Linux

Security_Severity-Low

Proj-xstream

Issue 50841: xstream:XmlFuzzer: Security exception in com.ctc.wstx.dtd.FullDTDReader.readContentSpec

Reported by [ClusterFuzz-External](#) on Wed, Aug 31, 2022, 5:55 PM EDT

Project Member

 Code

Detailed Report: <https://oss-fuzz.com/testcase?key=5060517357551616>

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/java.lang.ClassLoader.defineClass0

java.base/java.lang.System\$2.defineClass

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_asan_xstream&revision=202208310613

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5060517357551616

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 Thu, Sep 1, 2022, 11:08 AM EDT

Project Member

Status: Verified (was: New)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5060517357551616 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_xstream&range=202208310613:202209010605

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

[Comment 2](#) by [sheriffbot](#) on Wed, Sep 7, 2022, 2:53 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)