Starred by 1 user

Owner: ----

CC: t...@fasterxml.com
yak...@code-intelligence.com
fanni...@gmail.com
wag...@code-intelligence.com
da...@adalogics.com
patri...@code-intelligence.com
a...@adalogics.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-jackson-databind
Reported-2022-09-05

Issue 51020: jackson-databind:ObjectReader2Fuzzer: Security exception in com.fasterxml.jackson.databind.deser.std.StdDeserializer._parseBooleanPrimitive

Reported by ClusterFuzz-External on Mon, Sep 5, 2022, 10:22 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4650513269915648

Project: jackson-databind
Fuzzing Engine: libFuzzer
Fuzz Target: ObjectReader2Fuzzer
Job Type: libfuzzer_asan_jackson-databind
Platform Id: linux

Crash Type: Security exception
Crash Address:
Crash State:
  com.fasterxml.jackson.databind.deser.std.StdDeserializer._parseBooleanPrimitive
  java.base/sun.net.util.IPAddressUtil.checkHostString
  java.base/java.net.URLStreamHandler.setURL

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_jackson-databind&range=202209030612:202209040605

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4650513269915648

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 t...@fasterxml.com on Mon, Sep 5, 2022, 8:39 PM EDT

Valid, similarly to earlier findings for POJOs.

Reported as

Reported as

https://github.com/FasterXML/jackson-databind/issues/3590

to be addressed for `boolean` and other primitive types.

Comment 2 by ClusterFuzz-External on Wed, Sep 7, 2022, 10:11 AM EDT Project Member

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

ClusterFuzz testcase 4650513269915648 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_jackson-databind&range=202209060603:202209070610

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

Comment 3 by sheriffbot on Wed, Sep 7, 2022, 2:54 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot