☆ 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:	Aug 24, 2022
Type:	Bug-Security

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-Low
Proj-jackson-databind
Reported-2022-08-20
Disclosure-2022-11-18

Issue 50490: jackson-databind:ObjectReader2Fuzzer: Security exception in com.fasterxml.jackson.databind.deser.BeanDeserializer._deserializeFromArray

Reported by ClusterFuzz-External on Sat, Aug 20, 2022, 4:12 PM EDT   Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4681021680910336

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.BeanDeserializer._deserializeFromArray
  com.fasterxml.jackson.databind.deser.BeanDeserializer._deserializeOther
  com.fasterxml.jackson.databind.deser.BeanDeserializer.deserialize

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_jackson-databind&range=202208170610:202208180605

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4681021680910336

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 Sun, Aug 21, 2022, 2:53 PM EDT   Project Member

Labels: Disclosure-2022-11-18

Comment 2 by t...@fasterxml.com on Tue, Aug 23, 2022, 11:07 PM EDT

Interesting. I think this is valid concern.

Comment 3 by t...@fasterxml.com on Tue, Aug 23, 2022, 11:18 PM EDT

Filed

https://github.com/FasterXML/jackson-databind/issues/3582

and hoping this is easy to resolve (can't say off-hand if it is), but at least should be easy enough to write a unit test.

Comment 4 by t...@fasterxml.com on Tue, Aug 23, 2022, 11:56 PM EDT

And looks like it was fortunately easy enough to fix since look-ahead works in the specific spot (i.e. can look if the next token is `[`, fail in specific "unwrap-if-single-element" case). Should be fixed now.

Comment 5 by ClusterFuzz-External on Wed, Aug 24, 2022, 11:51 AM EDT Project Member

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

ClusterFuzz testcase 4681021680910336 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_jackson-databind&range=202208230604:202208240600

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

Comment 6 by sheriffbot on Wed, Aug 24, 2022, 2:44 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot