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: 9 days ago

Type: Bug-Security

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-Low
Proj-apache-commons-jxpath
ClusterFuzz-Good

Issue 47061: apache-commons-jxpath:JXPathFuzzer: Uncaught exception in org.apache.commons.jxpath.ri.compiler.CoreOperation.compute

Reported by ClusterFuzz-External on Wed, Apr 27, 2022, 9:18 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=6148152412995584

Project: apache-commons-jxpath
Fuzzing Engine: libFuzzer
Fuzz Target: JXPathFuzzer
Job Type: libfuzzer_asan_apache-commons-jxpath
Platform Id: linux

Crash Type: Uncaught exception
Crash Address:
Crash State:
  org.apache.commons.jxpath.ri.compiler.CoreOperation.compute
  org.apache.commons.jxpath.ri.compiler.CoreOperationCompare.equal
  org.apache.commons.jxpath.ri.compiler.CoreOperationCompare.computeValue

Sanitizer: address (ASAN)

Recommended Security Severity: Low

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_asan_apache-commons-jxpath&revision=202204270610

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=6148152412995584

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 Wed, Apr 27, 2022, 2:54 PM EDT Project Member

Labels: Disclosure-2022-07-26

Comment 2 by ClusterFuzz-External on Tue, May 17, 2022, 4:08 AM EDT Project Member

Labels: -Reported-2022-04-27 -Disclosure-2022-07-26

.

Comment 3 by ClusterFuzz-External on Wed, Jul 20, 2022, 10:15 AM EDT Project Member

Cc: h...@code-intelligence.com

Comment 4 by ClusterFuzz-External on Tue, Aug 16, 2022, 12:14 PM EDT Project Member

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

ClusterFuzz testcase 6148152412995584 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_apache-commons-jxpath&range=202208150608:202208160605

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

Comment 5 by sheriffbot on Tue, Aug 16, 2022, 2:40 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot

Comment 6 by ochang@google.com on Wed, Aug 17, 2022, 4:47 AM EDT Project Member

Status: New (was: Verified)

Possible infra issue. Re-opening out of caution.

Comment 7 by ochang@google.com on Wed, Aug 17, 2022, 5:55 AM EDT Project Member

Labels: Restrict-View-Commit

Comment 8 by ochang@google.com on Tue, Aug 23, 2022, 3:22 AM EDT Project Member

Labels: -ClusterFuzz-Verified

Comment 9 by ochang@google.com on Fri, Sep 16, 2022, 1:26 AM EDT Project Member

Labels: ClusterFuzz-Good

Comment 10 by ClusterFuzz-External on Wed, Sep 21, 2022, 10:56 AM EDT Project Member

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

ClusterFuzz testcase 6148152412995584 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_apache-commons-jxpath&range=202209200602:202209210607

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

Comment 11 by sheriffbot on Thu, Sep 22, 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

- Your friendly Sheriffbot

Comment 12 by sch...@gmail.com on Mon, Oct 10, 2022, 7:10 AM EDT

How can it be, that there is a CVE released to the public for this issue (https://nvd.nist.gov/vuln/detail/CVE-2022-40157) while there is no fix available AND the initiating issue (this one) states that the bug has been fixed?
Also, I can not see any activity of the maintainers of the JXPath project about such an issue.
Was the problem only in the testcases (oss-fuzz) and has been fixed there? Then you have a serious problem with your process...

Those oss-fuzz CVE issues are spamming our dependency checkers now with all sorts of "issues" where there is no fix available and obviously the maintainers even do not know yet that there are issues at all (if there are any at all).

Comment 13 by fanni...@gmail.com on Tue, Oct 11, 2022, 8:28 AM EDT

This issue was not responsibly disclosed to the Apache JXPath team. Google do not even have the right to publish CVEs for Apache projects. Apache is a CNA in its own right and it is up to them to publish CVEs for their projects.