Starred by 2 users

Owner:	----
CC:	bsh...@gmail.com yukih...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Aug 1, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Security_Severity-High
Proj-mruby
Engine-honggfuzz
Disclosure-2020-09-28
Reported-2020-06-30

Issue 23801: mruby:mruby_proto_fuzzer: Heap-double-free in mrb_default_allocf

Reported by ClusterFuzz-External on Tue, Jun 30, 2020, 3:49 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4894663076216832

Project: mruby
Fuzzing Engine: honggfuzz
Fuzz Target: mruby_proto_fuzzer
Job Type: honggfuzz_asan_mruby
Platform Id: linux

Crash Type: Heap-double-free
Crash Address: 0x60300001c8a0
Crash State:
  mrb_default_allocf
  mrb_free
  obj_free

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=honggfuzz_asan_mruby&range=202006070306:202006300453

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4894663076216832

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 Tue, Jun 30, 2020, 4:14 PM EDT Project Member

Labels: Disclosure-2020-09-28

Comment 2 by ClusterFuzz-External on Thu, Jul 2, 2020, 10:43 AM EDT Project Member

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

ClusterFuzz testcase 4894663076216832 is verified as fixed in https://oss-fuzz.com/revisions?job=honggfuzz_asan_mruby&range=202007010342:202007020339

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

Comment 3 by sheriffbot on Sat, Aug 1, 2020, 4:07 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot