Starred by 1 user

Owner: ----

CC: p.ant...@catenacyber.fr
sy...@lighttransport.com

Status: Verified *(Closed)*

Components: ----

Modified: Aug 30, 2022

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Unreproducible
Engine-libfuzzer
OS-Linux
Fuzz-Blocker
Security_Severity-High
Proj-tinygltf
Reported-2022-07-12

Issue 49053: tinygltf:fuzz_gltf: Command injection in tinygltf::ExpandFilePath

Reported by ClusterFuzz-External on Mon, Jul 11, 2022, 11:27 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5868065258078208

Project: tinygltf
Fuzzing Engine: libFuzzer
Fuzz Target: fuzz_gltf
Job Type: libfuzzer_asan_tinygltf
Platform Id: linux

Crash Type: Command injection
Crash Address:
Crash State:
  tinygltf::ExpandFilePath
  tinygltf::LoadExternalFile
  decltype

Sanitizer: address (ASAN)

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_asan_tinygltf&revision=202207110612

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5868065258078208

Issue manually filed by: ochang

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 ochang@google.com on Mon, Jul 11, 2022, 11:29 PM EDT Project Member

Note: the reproduction instructions for this aren't available yet, but hopefully the bug is clear from the stacktrace and the reproducer:

{"images":

[{"uri":"data:text/plain;base28,/AAAAAAEAAAASSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS+++++
++SSSSSSS/SSSSSSSSSSSS+++++++++++++++++
. . . . . SSSSSSSSSSSSSSS/Y///EoYYOAAAA

++SSSSSSSSSSSSSSSS//Y///EpYYQAAAA
AAAAAAAAAAEAAAAAAAQAAAAAAAAAAAAAAEAAAAAAQAAAAAAA____
____
_______________AAAAAAAEAAAAAA`AQAAAAAAAAAAAAQAAAAAAA`AAAAAAAEAAAAAAAAQAAAAAAA5"}],"ass
et":{"version":""}}

It seems anything passed between backticks (`) gets interpreted as a command to execute (due to the wordexp call). This does not seem to be part of the gltf spec: https://www.khronos.org/registry/glTF/specs/2.0/glTF-2.0.html

Comment 2 by sheriffbot on Tue, Jul 12, 2022, 2:56 PM EDT Project Member

Labels: Disclosure-2022-10-10

Comment 3 by ochang@google.com on Wed, Jul 13, 2022, 12:40 AM EDT Project Member

A more minimal PoC:

```
{"images":[{"uri":"a`echo iamhere > poc`"}], "asset":{"version":""}}
```

Comment 4 by ClusterFuzz-External on Wed, Jul 13, 2022, 7:06 AM EDT Project Member

Labels: Fuzz-Blocker

This crash occurs very frequently on linux platform and is likely preventing the fuzzer fuzz_gltf from making much progress. Fixing this will allow more bugs to be found.

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

Comment 5 by ochang@google.com on Tue, Aug 16, 2022, 2:59 AM EDT Project Member

Labels: -Restrict-View-Commit -Disclosure-2022-10-10

Derestricting as the upstream maintainer did not want to consider private reports (https://github.com/syoyo/tinygltf/issues/363, https://github.com/syoyo/tinygltf/issues/364)

Comment 6 by ochang@google.com on Tue, Aug 30, 2022, 12:13 AM EDT Project Member

Status: Verified (was: New)

Upstream bug with more details and fix: https://github.com/syoyo/tinygltf/issues/368