

[New issue](#)[Jump to bottom](#)

Command injection via wordexp call. #368

🔒 Closed

oliverchang opened this issue on Aug 16 · 6 comments

Labels

enhancement

oliverchang commented on Aug 16

Describe the issue

This is a security vulnerability. The `wordexp` call here allows arbitrary code execution

[tinygltf/tiny_gltf.h](#)
Line 2640 in 0fa56e2

```
2640      int ret = wordexp(quoted_path.c_str(), &p, 0);
```

when parsing a gltf file.

To Reproduce

- OS: Linux
- Compiler, compiler version, compile options: Clang 13.0.1-6

```
$ git clone https://github.com/syoyo/tinygltf
$ cd tinygltf && make all
$ echo '{"images":[{"uri":"a`echo iamhere > poc`"}], "asset":{"version":""}}' > payload.gltf
$ ./loader_example payload.gltf
$ cat poc
iamhere
```

Expected behaviour

The `echo iamhere > poc` command should not be executed and the `poc` file is not created in the CWD.

Additional context

This was found by OSS-Fuzz: <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=49053>

One potential fix here is to pass `WRDE_NOCMD` to `wordexp` per <https://man7.org/linux/man-pages/man3/wordexp.3.html>

syoyo commented on Aug 16

Owner

@oliverchang Thanks! In ExpandFilePath


[tinygltf/tiny_gltf.h](#)
Line 1266 in 0fa56e2

```
1266      std::string ExpandFilePath(const std::string &filepath, void *userdata);
```

wordexp is used to expand file path(i.e, expand environment variable, expand tilde(~) when a file path contains such symbol).

But according to glTF spec <https://registry.khronos.org/glTF/specs/2.0/glTF-2.0.html#uris> , uri must be URI/IRI, so file(resource) path should not contain environment variables and tilde, so we need to use URI decoder/encoder instead of ExpandFilePath .

Related: [#337](#)

 syoyo added the **enhancement** label on Aug 16

syoyo commented on Aug 16


Owner

Disabled file path expansion(so no wordexp anymore) in this commit: [52ff00a](#)

TODO: Proper/strict decoding/encoding of URI asset path:

[tinygltf/tiny_gltf.h](#)
Line 2202 in 9117abb

```
2202      // https://github.com/syoyo/tinygltf/issues/228
```

 syoyo closed this as completed on Aug 16

oliverchang commented on Aug 16 • edited ▼

Author

Thank you very much for the amazingly fast fix @syoyo !

Would it be possible to create a security advisory (and CVE) for this via <https://github.com/syoyo/tinygltf/security/advisories> so downstream users are notified? We (Google) can also help with this if you prefer.

syoyo commented on Aug 16

Owner

@oliverchang Oh, I didn't know Github has a Security page 🤔 Will take a look it.



DavidKorczynski mentioned this issue on Aug 16

plugins: refine function call analyser ossf/fuzz-introspector#473

Merged



This was referenced on Aug 16

Add query for tainted wordexp calls. github/codeql#10077

Merged

C/C++: Command injection via wordexp github/securitylab#700

Closed

oliverchang commented on Aug 23

Author

Hi @syoyo, have you had a chance to try generating an advisory for this issue? It's a crucial part of making sure users of this library are notified of vulnerabilities (and that they need to update).

oliverchang commented on Sep 5

Author

FYI we've requested CVE-2022-3008 for this vulnerability: <https://nvd.nist.gov/vuln/detail/CVE-2022-3008>

Assignees

No one assigned

Labels

enhancement

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

