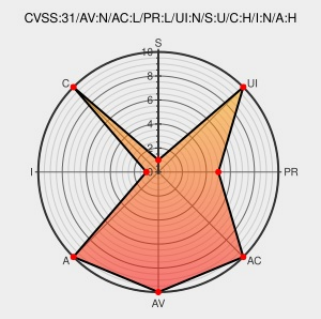
CVE-2022-3008

Published on: Not Yet Published

Last Modified on: 10/01/2022 02:17:00 AM UTC

CVE-2022-3008

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

The tinygltf library uses the C library function wordexp() to perform file path expansion on untrusted paths that are provided from the input file. This function allows for command injection by using backticks. An attacker could craft an untrusted path input that would result in a path expansion. We recommend upgrading to 2.6.0 or past commit 52ff00a38447f06a17eab1caa2cf0730a119c751

CVE-2022-3008 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **syoyo** - **tinygltf** version **< 2.6.0**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Command injection via wordexp call. · Issue #368 · syoyo/tinygltf · GitHub	github.com text/html	MISC github.com/syoyo/tinygltf/issues/368
Do not expand file path since its not necessary for glTF asset path(U… · syoyo/tinygltf@52ff00a · GitHub	github.com text/html	MISC github.com/syoyo/tinygltf/commit/52ff00a38447f06a17eab1caa2cf0730a119c751
49053 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=49053

Debian -- Security Information -- DSA-5232-1 tinygltf	www.debian.org Depreciated Link text/html	DEBIAN DSA-5232
tinygltf/README.md at master · syoyo/tinygltf · GitHub	github.com text/html	MISC github.com/syoyo/tinygltf/blob/master/README.md

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

181068 Debian Security Update for tinygltf (DSA 5232-1)

182396 Debian Security Update for tinygltf (CVE-2022-3008)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Tinygltf Project	Tinygltf	All	All	All	All

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:tinygltf_project:tinygltf:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3008 : The tinygltf library uses the C library function wordexp to perform file path expansion on untrus… twitter.com/i/web/status/1…	2022-09-05 09:17:18
/r/netcve	CVE-2022-3008	2022-09-05 09:38:46

← Previous ID

Next ID→