



CVE-2021-29562

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-29562
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-14 20:15:00 UTC
Updated	2021-05-18 20:07:00 UTC
Description	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by explc

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All

References

Reference	Source	Link	Tags
`CHECK`-fail in `tf.raw_ops.IRFFT` · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	github.com	
Fix a check fail in Fast Fourier implementation · tensorflow/tensorflow@1c56f53 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982487](#) Python (pip) Security Update for tensorflow-gpu (GHSA-36vm-xw34-x4pj)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report