CVE-2021-29584

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-29584
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	2021-05-20 15:38:00 UTC
Description	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `C

Risk And Classification

Problem Types: CWE-190

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
Prevent overflow in sparse op · tensorflow/tensorflow@4c0ee93 · GitHub	MISC	github.com	
`CHECK`-fail due to integer overflow · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	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

982469 Python (pip) Security Update for tensorflow-gpu (GHSA-xvjm-fvxx-q3hv)

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

CVE, CWE, and OVAL are registred 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.

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