



CVE-2021-41211

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

Summary

CVE	CVE-2021-41211
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-05 21:15:00 UTC
Updated	2021-11-09 15:14:00 UTC
Description	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `QuantizeV2`

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.6.0	All	All	All

References

Reference	Source	Link	Tags
Prevent OOB access in QuantizeV2 shape inference · tensorflow/tensorflow@a0d6444 · GitHub	MISC	github.com	
Heap OOB in shape inference for `QuantizeV2` · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980176](#) Python (pip) Security Update for tensorflow-gpu (GHSA-cvgx-3v3q-m36c)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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