CVE-2020-15196

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15196
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-25 19:15:00 UTC
Updated	2021-11-18 17:21:00 UTC
Description	In Tensorflow version 2.3.0, the `SparseCountSparseOutput` and `RaggedCountSparseOutput` implementations don't valid

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.3.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All

References

Reference	Source	Link	Tag
Fix multiple vulnerabilities in `tf.raw_ops.*CountSparseOutput`. · tensorflow/tensorflow@3cbb917 · GitHub	MISC	github.com	Patc
Heap buffer overflow in weighted sparse count ops · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	github.com	Expl
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	MISC	github.com	Thir
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980049 Python (pip) Security Update for tensorflow-gpu (GHSA-pg59-2f92-5cph)