



CVE-2020-15204

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

Summary

CVE	CVE-2020-15204
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	2021-09-16 15:45:00 UTC
Description	In eager mode, TensorFlow before versions 1.15.4, 2.0.3, 2.1.2, 2.2.1 and 2.3.1 does not set the session state. Hence, calling

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All

References

Reference	Source	Link	Tags
Segfault by calling session-only ops in eager mode · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	github.com	Exploit, Third Party
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	MISC	github.com	Third Party
Prevent segfault in `GetSessionHandle{,V2}` · tensorflow/tensorflow@9a133d7 · GitHub	MISC	github.com	Patch, Third Party
[security-announce] openSUSE-SU-2020:1766-1: moderate: Security update for	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, primary

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)