



CVE-2021-37678

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

Summary

CVE	CVE-2021-37678
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-12 23:15:00 UTC
Updated	2021-08-19 13:44:00 UTC
Description	TensorFlow is an end-to-end open source platform for machine learning. In affected versions TensorFlow and Keras can be

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.5.0	All	All	All
Application	Google	Tensorflow	2.6.0	rc0	All	All
Application	Google	Tensorflow	2.6.0	rc1	All	All
Application	Google	Tensorflow	2.6.0	rc2	All	All

References

Reference	Source	Link
Use the safer `safe_load` function instead of `unsafe_load` when poss... · tensorflow/tensorflow@23d6383 · GitHub	MISC	github.com
Arbitrary code execution due to YAML deserialization · Advisory · tensorflow/tensorflow · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981547](#) Python (pip) Security Update for tensorflow-gpu (GHSA-r6jx-9g48-2r5r)

© [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](#)