

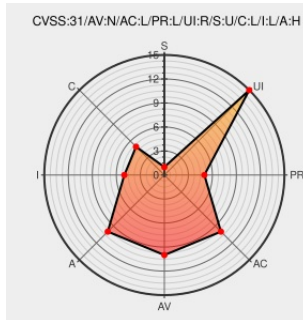


CVE-2022-41880

Published on: Not Yet Published

Last Modified on: 11/22/2022 09:52:00 PM UTC

CVE-2022-41880 - advisory for GHSA-8w5g-3wcv-9g2j

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` function receives a value in `true\_classes` larger than `range\_max`, a heap oob read occurs. We have patched the issue in GitHub commit

[b389f5c944cadfdfe599b3f1e4026e036f30d2d4](#). The fix will be included

in TensorFlow 2.11. We will also cherry-pick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.

CVE-2022-41880 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.10.0$, $< 2.10.1$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.9.0$, $< 2.9.3$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $< 2.8.4$

CVSS3 Score: **9.1 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	HIGH

CVE References

Description	Tags	Link
ThreadUnsafeUnigramCandidateSampler Heap OOB · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j

github.com/tensorflow/tensorflow/commit/b389f5c944cadfdfe599b3f1e4026e036f30

github.com/tensorflow/tensorflow/blob/master/tensorflow/core/kernels/candidate_sampler_ops.cc

[illegible]

904658 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (11524-1)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.10.0	All	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						
cpe:2.3:a:google:tensorflow:2.10.0:*:*:*:*:						

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-41880 : TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` func... twitter.com/i/web/status/1...	2022-11-18 21:18:24
 /r/netcve	CVE-2022-41880	2022-11-18 22:38:24

Next ID→

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