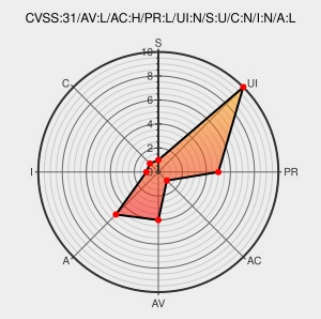
CVE-2021-29512

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 05/19/2021 09:09:00 PM UTC

CVE-2021-29512 - advisory for GHSA-4278-2v5v-65r4

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid

`SparseTensor`(https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from outside the bounds of the `splits` tensor buffer in the implementation of the `RaggedBincount` op(https://github.com/tensorflow/tensorflow/blob/8b677d79167799f71c42fd3fa074476e029541
L433). Before the `for` loop, `batch_idx` is set to 0. The user controls the `splits` array, making it contain only one element, 0. Thus, the code in the `while` loop would increment `batch_idx` and then try to read `splits(1)`, which is outside of bounds. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.

CVE-2021-29512 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>=2.3.0, < 2.3.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.4.0, < 2.4.2**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Heap buffer overflow in `RaggedBinCount` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-4278-2v5v-65r4
Fix an invalid address vulnerability in `tf.raw_ops.RaggedBincount`. · tensorflow/tensorflow@eebb96c · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/eebb96c2830d48597d055d247c0e9aebaea94cd5

Related QID Numbers

982534 Python (pip) Security Update for tensorflow-gpu (GHSA-4278-2v5v-65r4)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29512 : TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of… twitter.com/i/web/status/1…	2021-05-14 19:01:40
/r/netcve	CVE-2021-29512	2021-05-14 19:41:15

← Previous ID

Next ID→

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