



CVE-2021-29560

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

Last Modified on: 04/25/2022 08:04:00 PM UTC

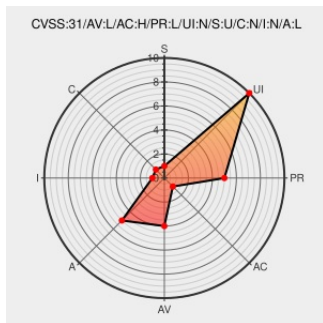
CVE-2021-29560 - advisory for GHSA-8gv3-57p6-g35r

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. An attacker can cause a heap buffer overflow in ``tf.raw_ops.RaggedTensorToTensor``. This is because the

implementation(<https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cL222>) uses the same index to access two arrays in parallel. Since the user controls the shape of the input arguments, an attacker could trigger a heap OOB access when ``parent_output_index`` is shorter than ``row_split``. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29560 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version < 2.1.4

Affected Vendor/Software: tensorflow - tensorflow version >= 2.2.0, < 2.2.3

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: **7.1 - HIGH**

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

CVSS2 Score: **3.6 - LOW**

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

CVE References

Description	Tags	Link
Heap buffer overflow in `RaggedTensorToTensor` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-8gv3-57p6-g35r
Fix heap-buffer-overflow issue with `tf.raw_ops.RaggedTensorToTensor`. · tensorflow/tensorflow@a84358a · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/a84358aa12f0b1518e606095ab9cfddb597c1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

982489 Python (pip) Security Update for tensorflow-gpu (GHSA-8gv3-57p6-g35r)

Known Affected Configurations (CPE V2.3)

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID→