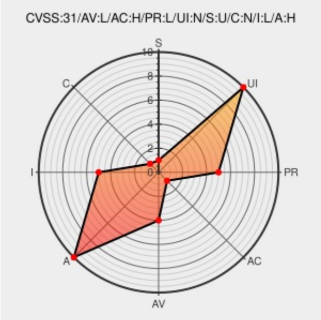
CVE-2021-29608

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

Last Modified on: 07/26/2021 04:23:00 PM UTC

CVE-2021-29608 - advisory for GHSA-rgvq-pcvf-hx75

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. Due to lack of validation in `tf.raw_ops.RaggedTensorToTensor`, an attacker can exploit an undefined behavior if input arguments are empty. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f
L360) only checks that one of the tensors is not empty, but does not check for the other ones. There are multiple `DCHECK` validations to prevent heap OOB, but these are no-op in release builds, hence they don't prevent anything. The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits 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-2021-29608 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: 7.8 - 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 OOB and null pointer dereference in `RaggedTensorToTensor` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-rgvq-pcvf-hx7
Fix heap OOB / undefined behavior in `RaggedTensorToTensor` · tensorflow/tensorflow@c4d7afb · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/c4d7afb6a5986b04505aca4466ae1951686c8
Fix `tf.raw_ops.RaggedTensorToTensor` failing CHECK. · tensorflow/tensorflow@b761c9b · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/b761c9b652af2107cfbc33efd19be0ce41daa33
Fix `tf.raw_ops.RaggedTensorToTensor` failing CHECK in `tensor.cc`. · tensorflow/tensorflow@f94ef35 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/f94ef358bb3e91d517446454edff6535bcfe8e4

Related QID Numbers

982446 Python (pip) Security Update for tensorflow-gpu (GHSA-rgvq-pcvf-hx75)

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→

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