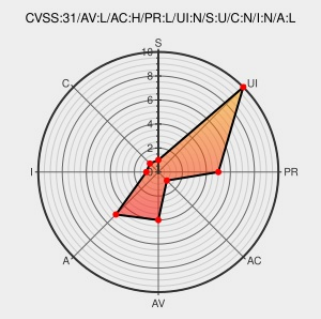
CVE-2021-29569

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

Last Modified on: 05/20/2021 02:56:00 PM UTC

CVE-2021-29569 - advisory for GHSA-3h8m-483j-7xxm

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. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ac328eaa3870491ababc147822c L50) assumes that the `input_min` and `input_max` tensors have at least one element, as it accesses the first element in two arrays. If the tensors are empty, `.flat<T>()` is an empty object, backed by an empty array. Hence, accesing even the 0th element is a read outside the bounds. 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-2021-29569 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
Fix out of bound read in requantization_range_op.cc · tensorflow/tensorflow@ef0c008 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/ef0c008ee84bad91ec6725ddc42091e19a30cf0e
Heap out of bounds read in `RequantizationRange` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-3h8m-483j-7xxm

Related QID Numbers

982480 Python (pip) Security Update for tensorflow-gpu (GHSA-3h8m-483j-7xxm)

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)

← Previous ID

Next ID→

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