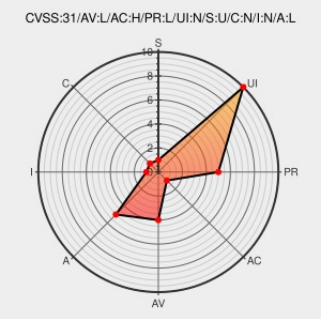
CVE-2021-29529

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

Last Modified on: 05/20/2021 04:26:00 PM UTC

CVE-2021-29529 - advisory for GHSA-jfp7-4j67-8r3q

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 trigger a heap buffer overflow in `tf.raw_ops.QuantizedResizeBilinear` by manipulating input values so that float rounding results in off-by-one error in accessing image elements. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e L66) computes two integers (representing the upper and lower bounds for interpolation) by ceiling and flooring a floating point value. For some values of `in`, `interpolation->upper[i]` might be smaller than `interpolation->lower[i]`. This is an issue if `interpolation->upper[i]` is capped at `in_size-1` as it means that `interpolation->lower[i]` points outside of the image. Then, in the interpolation code(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445 L264), this would result in heap buffer overflow. 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-2021-29529 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 buffer overflow caused by rounding · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-jfp7-4j67-8r3q
Fix heap buffer overflow caused by rounding. · tensorflow/tensorflow@f851613 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/f851613f8f0fb0c838d160ced13c134f778e3ce7

Related QID Numbers

982419 Python (pip) Security Update for tensorflow-gpu (GHSA-jfp7-4j67-8r3q)

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