

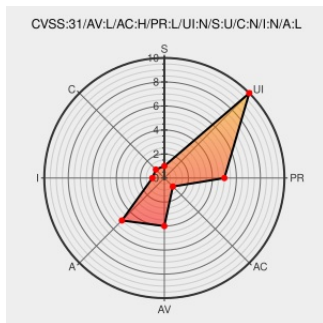


CVE-2021-29533

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

Last Modified on: 07/27/2021 05:30:00 PM UTC

CVE-2021-29533 - advisory for GHSA-393f-2jr3-cp69

[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 denial of service via a `CHECK` failure by passing an empty image to ``tf.raw_ops.DrawBoundingBoxes``. This is because the

implementation(<https://github.com/tensorflow/tensorflow/blob/ea34a18dc3f5c8d80a40ccca1404L165>) uses `CHECK\_\*` assertions instead of `OP\_REQUIRES` to validate user controlled inputs. Whereas `OP\_REQUIRES` allows returning an error condition back to the user, the `CHECK\_\*` macros result in a crash if the condition is false, similar to `assert`. In this case, `height` is 0 from the `images` input. This results in `max\_box\_row\_clamp` being negative and the assertion being falsified, followed by aborting program execution. 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-2021-29533 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** 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: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE

Score	Confidentiality	Integrity	Availability
-------	-----------------	-----------	--------------

Scope	Confidentiality Impact	Integrity Impact	Availability Impact			
UNCHANGED	NONE	NONE	HIGH			
CVSS2 Score: 2.1 - LOW						
Access Vector	Access Complexity	Authentication				
LOCAL	LOW	NONE				
Confidentiality Impact	Integrity Impact	Availability Impact				
NONE	NONE	PARTIAL				
CVE References						
Description	Tags	Link				
Fix overflow CHECK issue with <code>`tf.raw_ops.DrawBoundingBoxes`.</code> · tensorflow/tensorflow@b432a38 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/b432a38fe0e1b4b904a6c222cbce794c39703e87				
<code>`CHECK`</code> -fail in <code>`DrawBoundingBoxes`</code> · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-393f-2jr3-cp69				
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						
982515 Python (pip) Security Update for tensorflow-gpu (GHSA-393f-2jr3-cp69)						
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:*****:						

[illegible]

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID→		

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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