

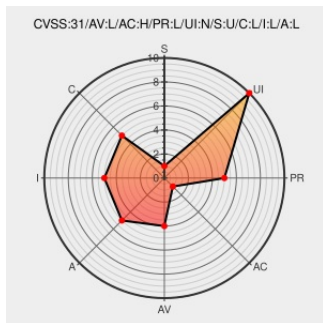


CVE-2021-29571

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

Last Modified on: 07/26/2021 04:10:00 PM UTC

CVE-2021-29571 - advisory for GHSA-whr9-vfh2-7hm6

[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/31bd5026304677faa8a0b77602cL130>) assumes that the last element of ``boxes`` input is 4, as required by [the op] (https://www.tensorflow.org/api_docs/python/tf/raw_ops/DrawBoundingBoxesV2). Since this is not checked attackers passing values less than 4 can write outside of bounds of heap allocated objects and cause memory corruption. If the last dimension in ``boxes`` is less than 4, accesses similar to ``tboxes(b, bb, 3)`` will access data outside of bounds. Further during code execution there are also writes to these indices. 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-2021-29571 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			
Fix memory corruption issue with `tf.raw_ops.DrawBoundingBoxesV2` · tensorflow/tensorflow@79865b5 · GitHub		github.com text/html		MISC github.com/tensorflow/tensorflow/commit/79865b542f9ffdc9caeb255631f7c56f1d4b6517			
Memory corruption in `DrawBoundingBoxesV2` · Advisory · tensorflow/tensorflow · GitHub		github.com text/html		CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-whr9-vfh2-7hm6			
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							
982478 Python (pip) Security Update for tensorflow-gpu (GHSA-whr9-vfh2-7hm6)							
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:*****:							

[illegible]

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-29571	2021-05-14 19:41:18

[← 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