

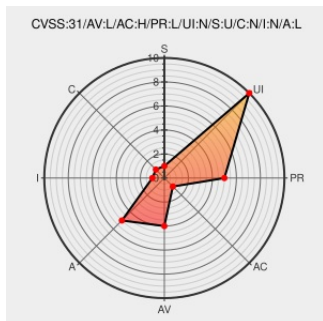


CVE-2021-29540

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

Last Modified on: 07/26/2021 04:03:00 PM UTC

CVE-2021-29540 - advisory for GHSA-xgc3-m89p-vr3x

[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 cause a heap buffer overflow to occur in `Conv2DBackpropFilter`. This is because the

implementation(<https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cdL497>) computes the size of the filter tensor but does not validate that it matches the number of elements in `filter\_sizes`. Later, when reading/writing to this buffer, code uses the value computed here, instead of the number of elements in the tensor. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick 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-2021-29540 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 issues in Conv2DBackpropFilter. · tensorflow/tensorflow@c570e2e · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/c570e2ecfc822941335ad48f6e10df4e21f11c96
Heap buffer overflow in `Conv2DBackpropFilter` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-xgc3-m89p-vr3x

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

982508 Python (pip) Security Update for tensorflow-gpu (GHSA-xgc3-m89p-vr3x)

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→		