

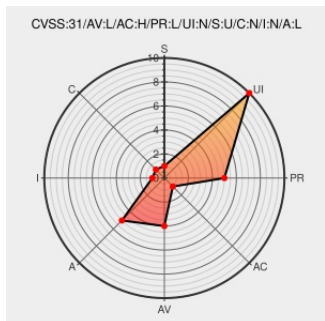


CVE-2021-29566

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

Last Modified on: 07/26/2021 04:20:00 PM UTC

CVE-2021-29566 - advisory for GHSA-pvrc-hg3f-58r6

[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 write outside the bounds of heap allocated arrays by passing invalid arguments to ``tf.raw_ops.Dilation2DBackpropInput``. This is because the

implementation(<https://github.com/tensorflow/tensorflow/blob/afd954e65f15aea4d438d0a21913L322>) does not validate before writing to the output array. The values for ``h_out`` and ``w_out`` are guaranteed to be in range for ``out_backprop`` (as they are loop indices bounded by the size of the array). However, there are no similar guarantees relating ``h_in_max``/``w_in_max`` and ``in_backprop``. 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-2021-29566 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 OOB access in `Dilation2DBackpropInput` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-pvrc-hg3f-58r6
Add missing validations in dillation ops. · tensorflow/tensorflow@3f6fe4d · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/3f6fe4dfef6f57e768260b48166c27d148f3015f

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

982483 Python (pip) Security Update for tensorflow-gpu (GHSA-pvrc-hg3f-58r6)

Known Affected Configurations (CPE V2.3)

[illegible]

```
cpe:2.3:a:google:tensorflow:*.:*:*:*:*:*:
```

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-2021-29566	2021-05-14 19:41:17

[← 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