

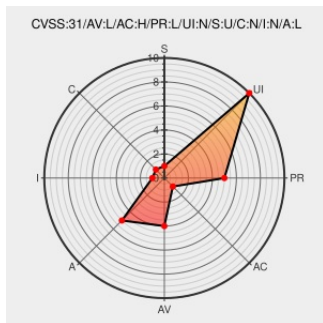


CVE-2021-29616

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

Last Modified on: 07/26/2021 04:21:00 PM UTC

CVE-2021-29616 - advisory for GHSA-4hvv-7x94-7vq8

[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

TrySimplify(<https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fc9aa7L401>) has undefined behavior due to dereferencing a null pointer in corner cases that result in optimizing a node with no inputs. 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-2021-29616 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

Access

Authentication

Vector	Complexity	
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Null dereference in Grappler's `TrySimplify` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-4hvv-7x94-7vq8
Handle a special grappler case resulting in crash. · tensorflow/tensorflow@e6340f0 · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/e6340f0665d53716ef3197ada88936c2a5f7a2d3

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

982439 Python (pip) Security Update for tensorflow-gpu (GHSA-4hvv-7x94-7vq8)

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:*:*:*:*:*:*:
```

```
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→