

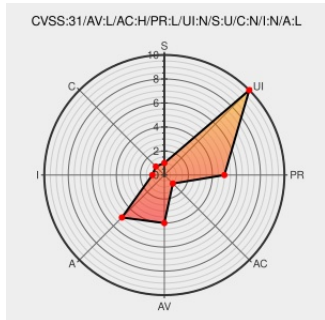


# CVE-2021-29516

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

Last Modified on: 05/20/2021 04:05:00 PM UTC

## CVE-2021-29516 - advisory for GHSA-84mw-34w6-2q43

[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. Calling `tf.raw_ops.RaggedTensorToVariant` with arguments specifying an invalid ragged tensor results in a null pointer dereference. The implementation of `RaggedTensorToVariant`

operations(<https://github.com/tensorflow/tensorflow/blob/904b3926ed1c6c70380d5313d282d24L40>) does not validate that the ragged tensor argument is non-empty. Since `batched_ragged` contains no elements, `batched_ragged.splits` is a null vector, thus `batched_ragged.splits(0)` will result in dereferencing `nullptr`. 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-2021-29516 has been assigned by [security-advisories@github.com](mailto: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    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

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<br>`tf.raw_ops.RaggedTensorToVariant`<br>invalid resize. ·<br>tensorflow/tensorflow@b055b9c ·<br>GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | MISC<br><a href="https://github.com/tensorflow/tensorflow/commit/b055b9c474cd376259dde8779908f9eef097d">github.com/tensorflow/tensorflow/commit/b055b9c474cd376259dde8779908f9eef097d</a> |
| Null pointer dereference via invalid<br>Ragged Tensors · Advisory ·<br>tensorflow/tensorflow · GitHub       | <a href="#">github.com</a><br><a href="#">text/html</a> | CONFIRM <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-84mw-34w6-2q43">github.com/tensorflow/tensorflow/security/advisories/GHSA-84mw-34w6-2q43</a>           |

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](mailto:comment@cve.report).

Related QID Numbers

982530 Python (pip) Security Update for tensorflow-gpu (GHSA-84mw-34w6-2q43)

Known Affected Configurations (CPE V2.3)

| Type        | Vendor | Product    | Version | Update | Edition | Language |
|-------------|--------|------------|---------|--------|---------|----------|
| Application | Google | Tensorflow | All     | All    | All     | All      |

cpe:2.3:a:google:tensorflow:\*:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

Social Mentions

| Source     | Title                                                                                                                                                                                                       | Posted (UTC)           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| @CVEreport | CVE-2021-29516 : TensorFlow is an end-to-end open source platform for machine learning. Calling<br>`tf.raw_ops.RaggedT... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-05-14<br>20:08:02 |
| /r/netcve  | <a href="#">CVE-2021-29516</a>                                                                                                                                                                              | 2021-05-14<br>20:41:08 |

[← 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](#)