

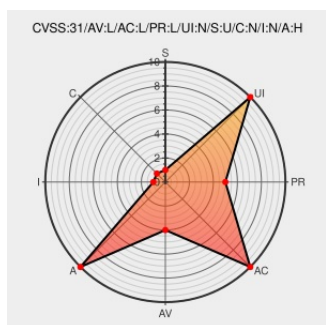


# CVE-2022-29197

Published on: Not Yet Published

Last Modified on: 05/26/2022 11:48:00 PM UTC

## CVE-2022-29197 - advisory for GHSA-hrg5-737c-2p56

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4, the implementation of ``tf.raw_ops.UnsortedSegmentJoin`` does not fully validate the input arguments. This results in a 'CHECK'-failure which can be used to trigger a denial of service attack. The code assumes ``num_segments``

is a scalar but there is no validation for this before accessing its value. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29197 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version < 2.6.4

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.7.0rc0, < 2.7.2

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.8.0rc0, < 2.8.1

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.9.0rc0, < 2.9.0

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 |
|---------------|-------------------|----------------|
| <b>LOCAL</b>  | <b>LOW</b>        | <b>NONE</b>    |

[illegible]

|                                                  |
|--------------------------------------------------|
| cpe:2.3:a:google:tensorflow:2.7.0:-:*:*:*:*:*:   |
| cpe:2.3:a:google:tensorflow:2.7.0:rc0:*:*:*:*:*: |
| cpe:2.3:a:google:tensorflow:2.7.0:rc1:*:*:*:*:*: |
| cpe:2.3:a:google:tensorflow:2.8.0:rc0:*:*:*:*:*: |
| cpe:2.3:a:google:tensorflow:2.8.0:rc1:*:*:*:*:*: |
| cpe:2.3:a:google:tensorflow:2.9.0:rc0:*:*:*:*:*: |
| cpe:2.3:a:google:tensorflow:2.9.0:rc1:*:*:*:*:*: |

No vendor comments have been submitted for this CVE

| Social Mentions                                                                              |                                                                                                                                                                                                                |                     |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Source                                                                                       | Title                                                                                                                                                                                                          | Posted (UTC)        |
|  @CVEreport  | CVE-2022-29197 : TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2,... <a href="https://twitter.com/i/web/status/1494444444">twitter.com/i/web/status/1...</a> | 2022-05-20 22:05:53 |
|  @LinInfoSec | Tensorflow - CVE-2022-29197: <a href="https://github.com/tensorflow/ten...">github.com/tensorflow/ten...</a>                                                                                                   | 2022-05-21 01:01:30 |
|  /r/netcve | <a href="#">CVE-2022-29197</a>                                                                                                                                                                                 | 2022-05-20 23:38:37 |