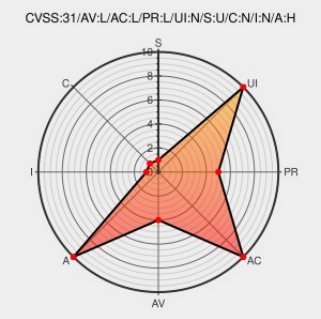
# CVE-2021-41196

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:18 PM UTC

## **CVE-2021-41196** - advisory for GHSA-m539-j985-hcr8

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. In affected versions the Keras pooling layers can trigger a segfault if the size of the pool is 0 or if a dimension is negative. This is due to the TensorFlow's implementation of pooling operations where the values in the sliding window are not checked to be strictly positive. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.

CVE-2021-41196 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.6.0, < 2.6.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.5.0, < 2.5.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.4.4**

### CVSS3 Score: 5.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 2.1 - LOW

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality** | **Integrity** | **Availability** |

| Confidentiality Impact | Integrity Impact | Availability Impact |
|---|---|---|
| NONE | NONE | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| tf.keras.layers.MaxPooling3D crashes · Issue #51936 · tensorflow/tensorflow · GitHub | github.com text/html | MISC github.com/tensorflow/tensorflow/issues/51936 |
| Merge pull request #51975 from yongtang:51936-max_pool3d · tensorflow/tensorflow@12b1ff8 · GitHub | github.com text/html | MISC github.com/tensorflow/tensorflow/commit/12b1ff82b3f26ff8de17e58703231d5a02ef1b8b |
| Crash in `max_pool3d` when size argument is 0 or negative · Advisory · tensorflow/tensorflow · GitHub | github.com text/html | CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-m539-j985-hcr8 |



## Related QID Numbers

980162 Python (pip) Security Update for tensorflow-gpu (GHSA-m539-j985-hcr8)

## 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-2021-41196 : TensorFlow is an open source platform for machine learning. In affected versions the Keras pooling… twitter.com/i/web/status/1… | 2021-11-05 20:00:25 |
| /r/msp | CVE-2021-41196 | 2021-11-09 15:00:32 |
| /r/Remotely_Alerts | CVE ID: CVE-2021-41196 | 2021-11-09 14:48:17 |

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**