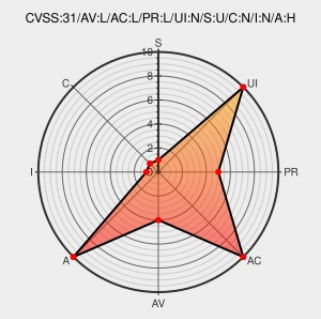
# CVE-2021-37686

Published on: 08/12/2021 12:00:00 AM UTC

Last Modified on: 08/18/2021 08:42:00 PM UTC

## **CVE-2021-37686** - advisory for GHSA-mhhc-q96p-mfm9

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. In affected versions the strided slice implementation in TFLite has a logic bug which can allow an attacker to trigger an infinite loop. This arises from newly introduced support for [ellipsis in axis definition] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/ L122). An attacker can craft a model such that `ellipsis_end_idx` is smaller than `i` (e.g., always negative). In this case, the inner loop does not increase `i` and the `continue` statement causes execution to skip over the preincrement at the end of the outer loop. We have patched the issue in GitHub commit dfa22b348b70bb89d6d6ec0ff53973bacb4f4695. TensorFlow 2.6.0 is the only affected version.

CVE-2021-37686 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**

### 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 |
|---|---|---|
| Prevent a division by 0 in average ops. · tensorflow/tensorflow@dfa22b3 · GitHub | github.com text/html | MISC github.com/tensorflow/tensorflow/commit/dfa22b348b70bb89d6d6ec0ff53973bacb4f4695 |
| Infinite loop in TFLite · Advisory · tensorflow/tensorflow · GitHub | github.com text/html | CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-mhhc-q96p-mfm9 |



## Related QID Numbers

981550 Python (pip) Security Update for tensorflow-gpu (GHSA-mhhc-q96p-mfm9)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Google | Tensorflow | All | All | All | All |
| Application | Google | Tensorflow | 2.5.0 | All | All | All |
| Application | Google | Tensorflow | 2.6.0 | rc0 | All | All |
| Application | Google | Tensorflow | 2.6.0 | rc1 | All | All |
| Application | Google | Tensorflow | 2.6.0 | rc2 | All | All |

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

cpe:2.3:a:google:tensorflow:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @LinInfoSec | Tensorflow - CVE-2021-37686: github.com/tensorflow/ten… | 2021-08-13 00:52:17 |

← Previous ID

Next ID→