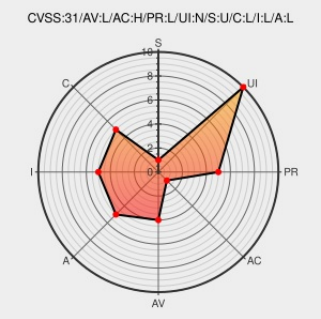
# CVE-2021-29571

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

Last Modified on: 07/26/2021 04:10:00 PM UTC

**CVE-2021-29571** - advisory for GHSA-whr9-vfh2-7hm6

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 `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/31bd5026304677faa8a0b77602c L130) assumes that the last element of `boxes` input is 4, as required by [the op] (https://www.tensorflow.org/api_docs/python/tf/raw_ops/DrawBoundingBoxesV2). Since this is not checked attackers passing values less than 4 can write outside of bounds of heap allocated objects and cause memory corruption. If the last dimension in `boxes` is less than 4, accesses similar to `tboxes(b, bb, 3)` will access data outside of bounds. Further during code execution there are also writes to these indices. 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-2021-29571 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** |

| Impact | Impact | Impact |
|---|---|---|
| UNCHANGED | HIGH | HIGH | HIGH |

## CVSS2 Score: 4.6 - MEDIUM

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

## CVE References

| Description | Tags | Link |
|---|---|---|
| Fix memory corruption issue with `tf.raw_ops.DrawBoundingBoxesV2`. · tensorflow/tensorflow@79865b5 · GitHub | github.com text/html | MISC github.com/tensorflow/tensorflow/commit/79865b542f9ffdc9caeb255631f7c56f1d4b6517 |
| Memory corruption in `DrawBoundingBoxesV2` · Advisory · tensorflow/tensorflow · GitHub | github.com text/html | CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-whr9-vfh2-7hm6 |



## Related QID Numbers

982478 Python (pip) Security Update for tensorflow-gpu (GHSA-whr9-vfh2-7hm6)

## Known Affected Configurations (CPE V2.3)

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

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) |
| --- | --- | --- |
| /r/netcve | CVE-2021-29571 | 2021-05-14 19:41:18 |

← Previous ID

Next ID→