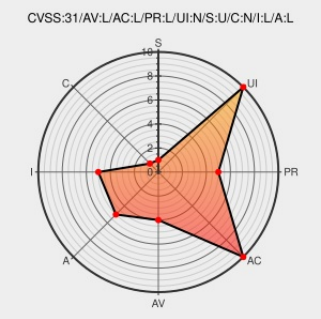
CVE-2020-26268

Published on: 12/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:57 PM UTC

CVE-2020-26268 - advisory for GHSA-hhvc-g5hv-48c6

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

In affected versions of TensorFlow the tf.raw_ops.ImmutableConst operation returns a constant tensor created from a memory mapped file which is assumed immutable. However, if the type of the tensor is not an integral type, the operation crashes the Python interpreter as it tries to write to the memory area. If the file is too small, TensorFlow properly returns an error as the memory area has fewer bytes than what is needed for the tensor it creates. However, as soon as there are enough bytes, the above snippet causes a segmentation fault. This is because the allocator used to return the buffer data is not marked as returning an opaque handle since the needed virtual method is not overridden. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.

CVE-2020-26268 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 1.15.5**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.0.0, < 2.0.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.1.0, < 2.1.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.2**

CVSS3 Score: 4.4 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
Mark `MemmappedTensorAllocator` as returning opaque handle. · tensorflow/tensorflow@c1e1fc8 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/commit/c1e1fc899ad5f8c725dcbb6470069890b5060
Write to immutable memory region · Advisory · tensorflow/tensorflow · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-hhvc-g5hv-48c6

Related QID Numbers

983226 Python (pip) Security Update for tensorflow-gpu (GHSA-hhvc-g5hv-48c6)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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