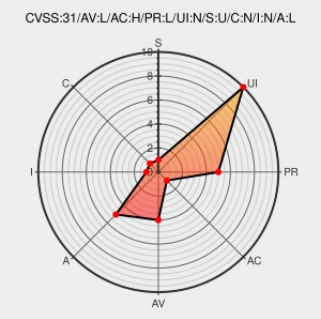
CVE-2021-29566

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

Last Modified on: 07/26/2021 04:20:00 PM UTC

CVE-2021-29566 - advisory for GHSA-pvrc-hg3f-58r6

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. An attacker can write outside the bounds of heap allocated arrays by passing invalid arguments to `tf.raw_ops.Dilation2DBackpropInput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/afd954e65f15aea4d438d0a21913L322) does not validate before writing to the output array. The values for `h_out` and `w_out` are guaranteed to be in range for `out_backprop` (as they are loop indices bounded by the size of the array). However, there are no similar guarantees relating `h_in_max`/`w_in_max` and `in_backprop`. 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-2021-29566 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**
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
Heap OOB access in `Dilation2DBackpropInput` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-pvrc-hg3f-58r6
Add missing validations in dillation ops. · tensorflow/tensorflow@3f6fe4d · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/3f6fe4dfef6f57e768260b48166c27d148f3015f

Related QID Numbers

982483 Python (pip) Security Update for tensorflow-gpu (GHSA-pvrc-hg3f-58r6)

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-2021-29566	2021-05-14 19:41:17

← Previous ID

Next ID→