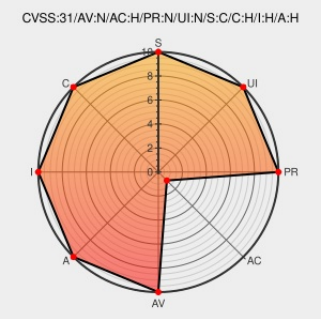
CVE-2020-15202

Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:26:00 PM UTC

CVE-2020-15202 - advisory for GHSA-h6fg-mjxg-hqq4

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



Certain versions of Tensorflow from Google contain the following vulnerability:

In Tensorflow before versions 1.15.4, 2.0.3, 2.1.2, 2.2.1 and 2.3.1, the `Shard` API in TensorFlow expects the last argument to be a function taking two `int64` (i.e., `long long`) arguments. However, there are several places in TensorFlow where a lambda taking `int` or `int32` arguments is being used. In these cases, if the amount of work to be parallelized is large enough, integer truncation occurs. Depending on how the two arguments of the lambda are used, this can result in segfaults, read/write outside of heap allocated arrays, stack overflows, or data corruption. The issue is patched in commits 27b417360cbd671ef55915e4bb6bb06af8b8a832 and ca8c013b5e97b1373b3bb1c97ea655e69f31a575, and is released in TensorFlow versions 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

CVE-2020-15202 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 1.15.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.0.0, < 2.0.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.1.0, < 2.1.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.1**

CVSS3 Score: 9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Prevent `int64` to `int` truncation in `Shard` API usage. · tensorflow/tensorflow@27b4173 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/commit/27b417360cbd671ef55915e4bb6bb06af8b8
Prevent integer truncation from 64 to 32 bits. · tensorflow/tensorflow@ca8c013 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/commit/ca8c013b5e97b1373b3bb1c97ea655e69f3
Integer truncation in Shard API usage · Advisory · tensorflow/tensorflow · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-h6fg-mjxg-
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.3.1
[security-announce] openSUSE-SU-2020:1766-1: moderate: Security update f	lists.opensuse.org, text/html	SUSE openSUSE-SU-2020:1766

Related QID Numbers

981469 Python (pip) Security Update for tensorflow-gpu (GHSA-h6fg-mjxg-hqq4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All

Application	Tensorflow	Tensorflow	All	All	All	All

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

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2020-15202: github.com/tensorflow/ten…	2021-09-16 19:45:19

← Previous ID

Next ID→