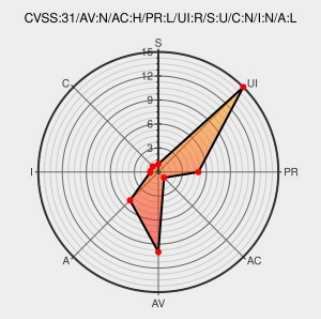
CVE-2019-16778

Published on: 12/16/2019 12:00:00 AM UTC

Last Modified on: 10/29/2021 03:03:00 PM UTC

CVE-2019-16778 - advisory for GHSA-844w-j86r-4x2j

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



Certain versions of Tensorflow from Google contain the following vulnerability:

In TensorFlow before 1.15, a heap buffer overflow in UnsortedSegmentSum can be produced when the Index template argument is int32. In this case data_size and num_segments fields are truncated from int64 to int32 and can produce negative numbers, resulting in accessing out of bounds heap memory. This is unlikely to be exploitable and was detected and fixed internally in TensorFlow 1.15 and 2.0.

CVE-2019-16778 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**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link

Description	Tags	Link
tensorflow/tfsa-2019-002.md at master · tensorflow/tensorflow · GitHub	Third Party Advisory github.com text/html	MISC github.com/tensorflow/tensorflow/blob/master/tensorflow/security/advisory/tfs 2019-002.md
Fix heap buffer overflow in UnsortedSegmentSum. · tensorflow/tensorflow@db4f971 · GitHub	Patch github.com text/html	MISC github.com/tensorflow/tensorflow/commit/db4f9717c41bccc3ce10099ab61996b24609
Heap buffer overflow in `UnsortedSegmentSum` · Advisory · tensorflow/tensorflow · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-844w-j86r-4

Related QID Numbers

980241 Python (pip) Security Update for tensorflow-gpu (GHSA-844w-j86r-4x2j)

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

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2019-16778: github.com/tensorflow/ten…	2021-10-29 16:46:26

← Previous ID

Next ID→

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