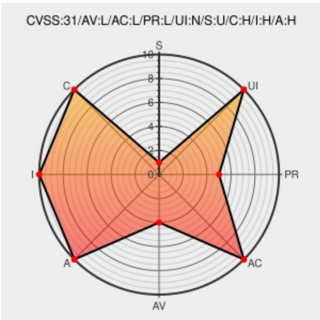
CVE-2021-41203

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 10/20/2022 09:36:00 PM UTC

CVE-2021-41203 - advisory for GHSA-7pxj-m4jf-r6h2

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



Certain versions of Tensorflow from Google contain the following vulnerability:

TensorFlow is an open source platform for machine learning. In affected versions an attacker can trigger undefined behavior, integer overflows, segfaults and `CHECK`-fail crashes if they can change saved checkpoints from outside of TensorFlow. This is because the checkpoints loading infrastructure is missing validation for invalid file formats. The fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.

CVE-2021-41203 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.6.0, < 2.6.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.5.0, < 2.5.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.4.4**

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**

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Prevent crashes when loading tensor slices with unsupported types. · tensorflow/tensorflow@abcced0 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/abcced051cb1bd8fb05046ac3b6023a7ebcc4578
Missing validation during checkpoint loading · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-7pxj-m4jf-r6h2
Use BuildTensorShapeBase when parsing unverified TensorShapes during … · tensorflow/tensorflow@b619c6f · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/b619c6f865715ca3b15ef1842b5b95edbaa710ad
Add BuildTensorSlice for building from unvalidated TensorSliceProtos. · tensorflow/tensorflow@e8dc637 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/e8dc63704c88007ee4713076605c90188d66f3d2
Avoid buffer overflow when loading tensors with insufficient data fro… · tensorflow/tensorflow@368af87 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/368af875869a204b4ac552b9ddda59f6a46a56ec

Related QID Numbers

980169 Python (pip) Security Update for tensorflow-gpu (GHSA-7pxj-m4jf-r6h2)

Exploit/POC from Github

TensorFlow is an open source platform for machine learning. In affected versions an attacker can trigger undefined be…

Known Affected Configurations (CPE V2.3)

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41203 : TensorFlow is an open source platform for machine learning. In affected versions an attacker can t… twitter.com/i/web/status/1…	2021-11-05 21:10:11