



CVE-2022-23558

Published on: 02/04/2022 12:00:00 AM UTC

Last Modified on: 02/09/2022 06:50:00 PM UTC

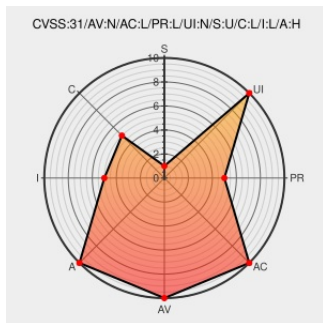
CVE-2022-23558 - advisory for GHSA-9gwq-6cwj-47h3

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause an integer overflow in `TfLiteIntArrayCreate`. The `TfLiteIntArrayGetSizeInBytes` returns an `int` instead of a `size\_t`. An attacker can control model inputs such that `computed\_size` overflows the size of `int` datatype. The fix will be

included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

CVE-2022-23558 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.7.0$, $< 2.7.1$

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.6.0$, $< 2.6.3$

Affected Vendor/Software: tensorflow - tensorflow version $< 2.5.3$

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

impact

PARTIAL

impact

PARTIAL

impact

PARTIAL

CVE References

Description	Tags	Link
tensorflow/common.c at ca6f96b62ad84207fbec580404eaa7dd7403a550 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/ca6f96b62ad84207fbec580404eaa7dd7403a550/tensorflow/common.c
tensorflow/common.c at ca6f96b62ad84207fbec580404eaa7dd7403a550 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/ca6f96b62ad84207fbec580404eaa7dd7403a550/tensorflow/common.c
Integer overflow in TFLite array creation · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-9c3d-4b3d-9c3d-4b3d
[lite] Update TfLiteIntArrayCreate to return size_t · tensorflow/tensorflow@a1e1511 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/a1e1511dde36b3f8aa27e1e1511dde36b3f8aa27e

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.7.0	All	All	All
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	All	All	All	All

cpe:2.3:a:google:tensorflow:2.7.0:*****:

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)
@CVEreport	CVE-2022-23558 : Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that... twitter.com/i/web/status/1...	2022-02-04 22:42:07
@LinInfoSec	Tensorflow - CVE-2022-23558: github.com/tensorflow/ten...	2022-02-05 02:00:14

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)