

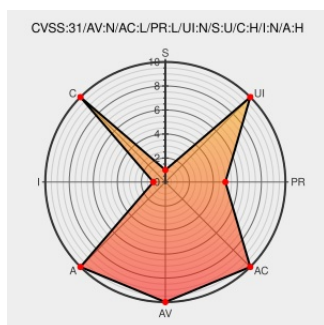


CVE-2022-23592

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

Last Modified on: 02/10/2022 02:18:00 AM UTC

CVE-2022-23592 - advisory for GHSA-vq36-27g6-p492

[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. TensorFlow's type inference can cause a heap out of bounds read as the bounds checking is done in a `DCHECK` (which is a no-op during production). An attacker can control the `input\_idx` variable such that `ix` would be larger than the number of values in `node\_t.args`. The fix will be included in TensorFlow 2.8.0. This is the only affected version.

CVE-2022-23592 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.7.0$, $< 2.8.0$

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Handle invalid inputs instead of crashing. · tensorflow/tensorflow@c99d98c · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/c99d98cd189839dcf51ae
tensorflow/graph.cc at 274df9b02330b790aa8de1cee164b70f72b9b244 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/274df9b02330b790aa8de1cee164b70f72b9b244/graph.cc#L229
Heap OOB access in `RunForwardTypeInference` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-vc

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	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-2022-23592 : Tensorflow is an Open Source Machine Learning Framework. TensorFlow's type inference can cause a h... twitter.com/i/web/status/1...	2022-02-04 22:52:37
@LinInfoSec	Tensorflow - CVE-2022-23592: github.com/tensorflow/ten...	2022-02-05 02:00:13
/r/netcve	CVE-2022-23592	2022-02-04 23:38:50

[← Previous ID](#)

[Next ID →](#)