

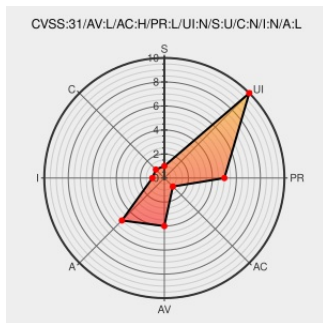


# CVE-2021-29574

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 05/18/2021 08:11:00 PM UTC

## CVE-2021-29574 - advisory for GHSA-828x-qc2p-wprq

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

TensorFlow is an end-to-end open source platform for machine learning. The implementation of ``tf.raw_ops.MaxPool3DGradGrad`` exhibits undefined behavior by dereferencing null pointers backing attacker-supplied empty tensors. The

implementation(<https://github.com/tensorflow/tensorflow/blob/72fe792967e7fd25234342068806L703>) fails to validate that the 3 tensor inputs are not empty. If any of them is empty, then accessing the elements in the tensor results in dereferencing a null pointer. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29574 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version < 2.1.4

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.2.0, < 2.2.3

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.3.0, < 2.3.3

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.4.0, < 2.4.2

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 |
| PARTIAL                | PARTIAL           | PARTIAL             |

### CVE References

| Description                                                                           | Tags                                                    | Link                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Undefined behavior in `MaxPool3DGradGrad` · Advisory · tensorflow/tensorflow · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | CONFIRM <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-828x-qc2p-wprq">github.com/tensorflow/tensorflow/security/advisories/GHSA-828x-qc2p-wprq</a>              |
| Add missing validation to pooling_ops_3d · tensorflow/tensorflow@a3d9f9b · GitHub     | <a href="#">github.com</a><br><a href="#">text/html</a> | MISC <a href="https://github.com/tensorflow/tensorflow/commit/a3d9f9be9ac2296615644061b40cefcee341dcc4">github.com/tensorflow/tensorflow/commit/a3d9f9be9ac2296615644061b40cefcee341dcc4</a> |

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](mailto:comment@cve.report).

### Related QID Numbers

982475 Python (pip) Security Update for tensorflow-gpu (GHSA-828x-qc2p-wprq)

### Known Affected Configurations (CPE V2.3)

| Type                                   | Vendor                 | Product                    | Version | Update | Edition | Language |
|----------------------------------------|------------------------|----------------------------|---------|--------|---------|----------|
| Application                            | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 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)        |
|-----------|--------------------------------|---------------------|
| /r/netcve | <a href="#">CVE-2021-29574</a> | 2021-05-14 19:41:20 |

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](#)