

Type confusion leading to `CHECK`-failure based denial of service

Low mihairmaruseac published GHSA-f4rr-5m7v-wxcw on May 17

Package

 tensorflow, tensorflow-cpu, tensorflow-gpu (pip)

Affected versions

< 2.9.0

Patched versions

2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

The [macros that TensorFlow uses for writing assertions](#) (e.g., `CHECK_LT`, `CHECK_GT`, etc.) have an incorrect logic when comparing `size_t` and `int` values. Due to type conversion rules, several of the macros would trigger incorrectly.

Patches

We have patched the issue in GitHub commit [b917181c29b50cb83399ba41f4d938dc369109a1](#) (merging GitHub PR [#55730](#)).

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, as these are also affected and still in supported range.

For more information

Please consult [our security guide](#) for more information regarding the security model and how to contact us with issues and questions.

Attribution

This vulnerability has been reported externally via a [GitHub issue](#).

Severity

Low

CVE ID

CVE-2022-29209

Weaknesses

No CWEs