Null dereference in Grappler's `TrySimplify`

Low **mihaimaruseac** published **GHSA-4hvv-7x94-7vq8** on May 12, 2021

Package

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

Affected versions	Patched versions
< 2.5.0	2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

The implementation of `TrySimplify` has undefined behavior due to dereferencing a null pointer in corner cases that result in optimizing a node with no inputs.

Patches

We have patched the issue in GitHub commit e6340f0665d53716ef3197ada88936c2a5f7a2d3.

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.

For more information

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

Severity

Low

CVE ID

CVE-2021-29616

Weaknesses

No CWEs