Heap out of bounds read in filesystem glob matching

Critical mihaimaruseac published **GHSA-9jjw-hf72-3mxw** on Dec 9, 2020

Package

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

Affected versions	Patched versions
2.4.0rc*	2.4.0

Description

Impact

The general implementation for matching filesystem paths to globbing pattern is vulnerable to an access out of bounds of the array holding the directories:

```
if (!fs->Match(child_path, dirs[dir_index])) { ... }
```

Since `dir_index` is unconditionaly incremented outside of the lambda function where the vulnerable pattern occurs, this results in an access out of bounds issue under certain scenarios. For example, if `/tmp/x` is a directory that only contains a single file `y`, then the following scenario will cause a crash due to the out of bounds read:

```
>>> tf.io.gfile.glob('/tmp/x/')
Segmentation fault
```

There are multiple invariants and preconditions that are assumed by the parallel implementation of `GetMatchingPaths` but are not verified by the PRs introducing it (#40861 and #44310). Thus, we are completely rewriting the implementation to fully specify and validate these.

Patches

We have patched the issue in GitHub commit 8b5b9dc96666a3a5d27fad7179ff215e3b74b67c and will release TensorFlow 2.4.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved.

This issue only impacts master branch and the release candidates for TF version 2.4. The final release of the 2.4 release will be patched.

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 by members of the Aivul Team from Qihoo 360.

Severity

Critical

CVE ID

CVE-2020-26269

Weaknesses

No CWEs