# CVE Detail – CVE-2021-29529

TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in `tf.raw\_ops.QuantizedResizeBilinear` by manipulating input values so that float rounding results in off-by-one error in accessing image elements. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized\_resize\_bilinear\_op.cc#L62-L66) computes two integers (representing the upper and lower bounds for interpolation) by ceiling and flooring a floating point value. For some values of `in`, `interpolation->upper[i]` might be smaller than `interpolation->lower[i]`. This is an issue if `interpolation->upper[i]` is capped at `in\_size-1` as it means that `interpolation->lower[i]` points outside of the image. Then, in the interpolation code(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized\_resize\_bilinear\_op.cc#L245-L264), this would result in heap buffer overflow. 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.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.14274

## CVSS Scoring

CVSS v3.1 Score: 2.5

Severity: LOW

## Mapped CWE(s)

* CWE-131: Incorrect Calculation of Buffer Size
* CWE-193: Off-by-one Error

## CAPEC(s)

* CAPEC-100: Overflow Buffers
* CAPEC-47: Buffer Overflow via Parameter Expansion

## Affected Products

* cpe:2.3:a:google:tensorflow:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:google:tensorflow:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:google:tensorflow:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:google:tensorflow:\*:\*:\*:\*:\*:\*:\*:\*