Vulnerability Summary for the Week of May 17, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cars-seller-auto-classifieds-script_project -- cars-seller-auto-classifieds-script	The request_list_request AJAX call of the Car Seller - Auto Classifieds Script WordPress plugin through 2.1.0, available to both authenticated and unauthenticated users, does not sanitise, validate or escape the order_id POST parameter before using it in a SQL statement, leading to a SQL Injection issue.	2021-05-14	7.5	CVE-2021-24285 MISC CONFIRM
kaswara_project -- kaswara	The Kaswara Modern VC Addons WordPress plugin through 3.0.1 allows unauthenticated arbitrary file upload via the 'uploadFontIcon' AJAX action. The supplied zipfile being	2021-05-14	7.5	CVE-2021-24284

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unzipped in the wp-content/uploads/kaswara/fonts_icon directory with no checks for malicious files such as PHP.			MISC CONFIRM
laobancms -- laobancms	Unrestricted File Upload in LAOBANCMS v2.0 allows remote attackers to upload arbitrary files by attaching a file with a ".jpg.php" extension to the component "admin/wenjian.php?wj=../templets/pc".	2021-05-14	7.5	CVE-2020-18166 MISC
linux -- linux_kernel	The block subsystem in the Linux kernel before 5.2 has a use-after-free that can lead to arbitrary code execution in the kernel context and privilege escalation, aka CID-c3e2219216c9. This is related to blk_mq_free_rqs and blk_cleanup_queue.	2021-05-14	7.2	CVE-2019-25044 MISC MISC MISC MISC
yfcmf -- yfcmf	YFCMF v2.3.1 has a Remote Command Execution (RCE) vulnerability in the index.php.	2021-05-14	7.5	CVE-2020-23691 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.69 was vulnerable to Reflected Cross-Site Scripting (XSS) issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users)	2021-05-14	4.3	CVE-2021-24291 MISC CONFIRM
apache -- traffic_server	Apache Traffic Server 9.0.0 is vulnerable to a remote DOS attack on the experimental Slicer plugin.	2021-05-14	5	CVE-2021-27737 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST MLIST
dedecms -- dedecms	DedeCMS V5.7 SP2 contains a CSRF vulnerability that allows a remote attacker to send a malicious request to to the web manager allowing remote code execution.	2021-05-15	6.8	CVE-2021-32073 MISC
express_handlebars_project -- express_handlebars	Express-handlebars is a Handlebars view engine for Express. Express-handlebars mixes pure template data with engine configuration options through the Express render API. More specifically, the layout parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only files with existing extentions (i.e. file.extension) can be included, files that lack an extension will have .handlebars appended to them. For complete	2021-05-14	5	CVE-2021-32820 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	details refer to the referenced GHSL-2021-018 report. Notes in documentation have been added to help users avoid this potential information exposure vulnerability.			RM MISC MISC MISC MISC
express_handlebars_project -- express_handlebars	express-hbs is an Express handlebars template engine. express-hbs mixes pure template data with engine configuration options through the Express render API. More specifically, the layout parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only files with existing extentions (i.e. file.extension) can be included, files that lack an extension will have .hbs appended to them. For complete details refer to the referenced GHSL-2021-019 report. Notes in documentation have been added to help users of express-hbs avoid this potential information exposure vulnerability.	2021-05-14	4.3	CVE-2021-32817 MISC CONFIRM MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				C MIS C
gnu -- libredwg	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_read_B ../../src/bits.c:135.	2021-05-17	6.8	CVE-2020-21841 MIS C MIS C MIS C
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:48.	2021-05-17	6.8	CVE-2020-218

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				18 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_revhistory ../../src/decode.c:3051.	2021-05-17	6.8	CVE-2020-21842 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulneraibility exists in GNU LibreDWG 0.10 via bit_calc_CRC ../../src/bits.c:2213.	2021-05-17	6.8	CVE-2020-218

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				30 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2417.	2021-05-17	6.8	CVE-2020-21832 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via: read_2004_section_classes ../../src/decode.c:2440.	2021-05-17	6.8	CVE-2020-218

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				33 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_preview ../../src/decode.c:3175.	2021-05-17	6.8	CVE-2020-21836 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_search_sentinel ../../src/bits.c:1985.	2021-	6.8	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		05-17		0-21840 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via: read_2004_section_appinfo ../../src/decode.c:2842.	2021-05-17	6.8	CVE-2020-21838 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641via htmlescape ../../programs/escape.c:51.	2021-05-17	6.8	CVE-2020-21819 MISC MISC
gnu -- libredwg	A heab based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:46.	2021-05-17	6.8	CVE-2020-21816 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.10. Crafted input will lead to an memory leak in dwg_decode_eed ../../src/decode.c:3638.	2021-05-17	4.3	CVE-2020-21839 MISC MISC
gnu -- libredwg	A null pointer deference issue exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2337.	2021-05-17	4.3	CVE-2020-21835 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	A null pointer deference issue exists in GNU LibreDWG 0.10 via get_bmp ../../programs/dwgbmp.c:164.	2021-05-17	4.3	CVE-2020-21834 MISC MISC
gnu -- libredwg	A null pointer dereference issue exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:29. which causes a denial of service (application crash).	2021-05-17	4.3	CVE-2020-21817 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	A null pointer deference issue exists in GNU LibreDWG 0.10.2641 via output_TEXT ../../programs/dwg2SVG.c:114, which causes a denial of service (application crash).	2021-05-17	4.3	CVE-2020-21815 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_read_RC ../../src/bits.c:318.	2021-05-17	6.8	CVE-2020-21843 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via htmlwescape ../../programs/escape.c:97.	2021-05-17	6.8	CVE-2020-21814 MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `MatrixDiag*` operations(https://github.com/tensorflow/tensorflow/blob/4c4f420e68f1cfaf8f4b6e8e3eb857e9e4c3ff33/tensorflow/core/kernels/linalg/matrix_diag_op.cc#L195-L197) does not validate that the tensor arguments are non-empty. 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.	2021-05-14	4.6	CVE-2021-29515 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropInput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/b40060c9f697b044e3107917c797ba052f4506ab/tensorflow/core/kernels/conv_grad_input_ops.h#L625-L655) does a division by a quantity that is controlled by the caller. 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.	2021-05-14	4.6	CVE-2021-29525 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Missing validation between arguments to `tf.raw_ops.Conv3DBackprop*` operations can result in heap buffer overflows. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/4814fafb0ca6b5ab58a09411523b2193fed23fed/tensorflow/core/kernels/conv_grad_shape_utils.cc#L94-L153) assumes that the `input`, `filter_sizes` and `out_backprop` tensors have the same shape, as they are accessed in parallel. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2,	2021-05-14	4.6	CVE-2021-29520 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.			NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. In eager mode (default in TF 2.0 and later), session operations are invalid. However, users could still call the raw ops associated with them and trigger a null pointer dereference. The implementation(https://github.com/tensorflow/tensorflow/blob/eebb96c2830d48597d055d247c0e9aebaea94cd5/tensorflow/core/kernels/session_ops.cc#L104) dereferences the session state pointer without checking if it is valid. Thus, in eager mode, `ctx->session_state()` is nullptr and the call of the member function is undefined behavior. 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.	2021-05-14	4.6	CVE-2021-29518 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGrad` is vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/ab1e644b48c82cb71493f4362b4dd38f4577a1cf/tensorflow/core/kernels/ma	2021-05-14	4.6	CVE-2021-295

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	xpooling_op.cc#L194-L203) fails to validate that indices used to access elements of input/output arrays are valid. Whereas accesses to `input_backprop_flat` are guarded by `FastBoundsCheck`, the indexing in `out_backprop_flat` can result in OOB access. 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.			79 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor`(https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from outside the bounds of the `splits` tensor buffer in the implementation of the `RaggedBincount` op(https://github.com/tensorflow/tensorflow/blob/8b677d79167799f71c42fd3fa074476e0295413a/tensorflow/core/kernels/bincount_op.cc#L430-L446). Before the `for` loop, `batch_idx` is set to 0. The attacker sets `splits(0)` to be 7, hence the `while` loop does not execute and `batch_idx` remains 0. This then results in writing to `out(-1, bin)`, which is before the heap allocated buffer for the output	2021-05-14	4.6	CVE-2021-29514 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedMul` by passing in invalid thresholds for the quantization. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/87cf4d3ea9949051e50ca3f071fc909538a51cd0/tensorflow/core/kernels/quantized_mul_op.cc#L287-L290) assumes that the 4 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an empty buffer and accessing the element at position 0 results in 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.	2021-05-14	4.6	CVE-2021-29535 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.AvgPool3DGrad` is vulnerable to a heap buffer overflow. The	2021-	4.6	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/d80ffba9702dc19d1fac74fc4b766b3fa1ee976b/tensorflow/core/kernels/pooling_ops_3d.cc#L376-L450) assumes that the `orig_input_shape` and `grad` tensors have similar first and last dimensions but does not check that this assumption is validated. 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.	05-14		1-29577 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference by providing an invalid `permutation` to `tf.raw_ops.SparseMatrixSparseCholesky`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/kernels/sparse/sparse_cholesky_op.cc#L85-L86) fails to properly validate the input arguments. Although `ValidateInputs` is called and there are checks in the body of this function, the code proceeds to the next line in `ValidateInputs` since `OP_REQUIRES`(https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/framewor	2021-05-14	4.6	CVE-2021-29530 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	k/op_requires.h#L41-L48) is a macro that only exits the current function. Thus, the first validation condition that fails in `ValidateInputs` will cause an early return from that function. However, the caller will continue execution from the next line. The fix is to either explicitly check `context->status()` or to convert `ValidateInputs` to return a `Status`. 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.			
google -- tensorflow	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-	2021-05-14	4.6	CVE-2021-29529 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>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.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor`(https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from outside the bounds of the `splits` tensor buffer in the implementation of the `RaggedBincount` op(https://github.com/tensorflow/tensorflow/blob/8b677d79167799f71c42fd3fa074476e0295413a/tensorflow/core/kernels/bincount_op.cc#L430-L433). Before the `for` loop, `batch_idx` is set to 0. The user controls the `splits` array, making it contain only one element, 0.	2021-05-14	4.6	CVE-2021-29512 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Thus, the code in the `while` loop would increment `batch_idx` and then try to read `splits(1)`, which is outside of bounds. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedReshape` by passing in invalid thresholds for the quantization. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a324ac84e573fba362a5e53d4e74d5de6729933e/tensorflow/core/kernels/quantized_reshape_op.cc#L38-L55) assumes that the 2 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an empty buffer and accessing the element at position 0 results in 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.	2021-05-14	4.6	CVE-2021-29536 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPool3DGradGrad` is	2021-	4.6	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/596c05a159b6fbb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/pooling_ops_3d.cc#L694-L696) does not check that the initialization of `Pool3dParameters` completes successfully. Since the constructor(https://github.com/tensorflow/tensorflow/blob/596c05a159b6fbb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/pooling_ops_3d.cc#L48-L88) uses `OP_REQUIRES` to validate conditions, the first assertion that fails interrupts the initialization of `params`, making it contain invalid data. In turn, this might cause a heap buffer overflow, depending on default initialized values. 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.	05-14		2021-29576 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedResizeBilinear` by passing in invalid thresholds for the quantization. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/50711818d2e61ccce012591eeb4fdf93a8496726/tensorflow/core/kernels/qua	2021-05-14	4.6	CVE-2021-29537

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ntized_resize_bilinear_op.cc#L705-L706) assumes that the 2 arguments are always valid scalars and tries to access the numeric value directly. 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.			CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow to occur in `Conv2DBackpropFilter`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv_grad_filter_ops.cc#L495-L497) computes the size of the filter tensor but does not validate that it matches the number of elements in `filter_sizes`. Later, when reading/writing to this buffer, code uses the value computed here, instead of the number of elements in the tensor. 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.	2021-05-14	4.6	CVE-2021-29540 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger an integer division by zero undefined behavior in `tf.raw_ops.QuantizedBiasAdd`. This is because the implementation of the Eigen kernel(https://github.com/tensorflow/tensorflow/blob/61bca8bd5ba8a68b2d97435ddfafcdf2b85672cd/tensorflow/core/kernels/quantization_utils.h#L812-L849) does a division by the number of elements of the smaller input (based on shape) without checking that this is not zero. 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.	2021-05-14	4.6	CVE-2021-29546 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.SparseSplit`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/699bff5d961f0abfde8fa3f876e6d241681fbef8/tensorflow/core/util/sparse/sparse_tensor.h#L528-L530) accesses an array element based on a user controlled offset. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow	2021-05-14	4.6	CVE-2021-29558 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.			MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can write outside the bounds of heap allocated arrays by passing invalid arguments to `tf.raw_ops.Dilation2DBackpropInput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/afd954e65f15aea4d438d0a219136fc4a63a573d/tensorflow/core/kernels/dilation_ops.cc#L321-L322) does not validate before writing to the output array. The values for `h_out` and `w_out` are guaranteed to be in range for `out_backprop` (as they are loop indices bounded by the size of the array). However, there are no similar guarantees relating `h_in_max`/`w_in_max` and `in_backprop`. 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.	2021-05-14	4.6	CVE-2021-29566 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger undefined behavior by binding to null pointer in `tf.raw_ops.ParameterizedTruncatedNormal`. This is	2021-	4.6	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because the implementation(https://github.com/tensorflow/tensorflow/blob/3f6fe4dfef6f57e768260b48166c27d148f3015f/tensorflow/core/kernels/parameterized_truncated_normal_op.cc#L630) does not validate input arguments before accessing the first element of `shape`. If `shape` argument is empty, then `shape_tensor.flat<T>()` is an empty array. 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.	05-14		1-29568 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/31bd5026304677faa8a0b77602c6154171b9aec1/tensorflow/core/kernels/image/draw_bounding_box_op.cc#L116-L130) assumes that the last element of `boxes` input is 4, as required by [the op](https://www.tensorflow.org/api_docs/python/tf/raw_ops/DrawBoundingBoxesV2). Since this is not checked attackers passing values	2021-05-14	4.6	CVE-2021-29571 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	less than 4 can write outside of bounds of heap allocated objects and cause memory corruption. If the last dimension in `boxes` is less than 4, accesses similar to `tboxes(b, bb, 3)` will access data outside of bounds. Further during code execution there are also writes to these indices. 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.			
google -- tensorflow	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/72fe792967e7fd25234342068806707bbc116618/tensorflow/core/kernels/pooling_ops_3d.cc#L679-L703) 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.	2021-05-14	4.6	CVE-2021-29574 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of TrySimplify(https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fc9aa74ed79595/tensorflow/core/grappler/optimizers/arithmetic_optimizer.cc#L390-L401) has undefined behavior due to dereferencing a null pointer in corner cases that result in optimizing a node with no inputs. 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.	2021-05-14	4.6	CVE-2021-29616 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The validation in `tf.raw_ops.QuantizeAndDequantizeV2` allows invalid values for `axis` argument:. The validation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L74-L77) uses `||` to mix two different conditions. If `axis_ < -1` the condition in `OP_REQUIRES` will still be true, but this value of `axis_` results in heap underflow. This allows attackers to read/write to other data on the heap. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit	2021-05-14	4.6	CVE-2021-29610 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Calling TF operations with tensors of non-numeric types when the operations expect numeric tensors result in null pointer dereferences. The conversion from Python array to C++ array(https://github.com/tensorflow/tensorflow/blob/ff70c47a396ef1e3cb73c90513da4f5cb71bebba/tensorflow/python/lib/core/ndarray_tensor.cc#L113-L169) is vulnerable to a type confusion. 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.	2021-05-14	4.6	CVE-2021-29513 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.io.decode_raw` produces incorrect results and crashes the Python interpreter when combining `fixed_length` and wider datatypes. The implementation of the padded version(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167	2021-05-14	4.6	CVE-2021-29614

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc) is buggy due to a confusion about pointer arithmetic rules. First, the code computes(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L61) the width of each output element by dividing the `fixed_length` value to the size of the type argument. The `fixed_length` argument is also used to determine the size needed for the output tensor(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L63-L79). This is followed by reencoding code(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L85-L94). The erroneous code is the last line above: it is moving the `out_data` pointer by `fixed_length * sizeof(T)` bytes whereas it only copied at most `fixed_length` bytes from the input. This results in parts of the input not being decoded into the output. Furthermore, because the pointer advance is far wider than desired, this quickly leads to writing to outside the bounds of the backing data. This OOB write leads to interpreter crash in the reproducer mentioned here, but more severe attacks can be mounted too, given that this gadget allows writing to periodically placed locations in memory. The			MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FusedBatchNorm` is vulnerable to a heap buffer overflow. If the tensors are empty, the same implementation can trigger undefined behavior by dereferencing null pointers. The implementation(https://github.com/tensorflow/tensorflow/blob/57d86e0db5d1365f19adcce848dfc1bf89fdd4c7/tensorflow/core/kernels/fused_batch_norm_op.cc) fails to validate that `scale`, `offset`, `mean` and `variance` (the last two only when required) all have the same number of elements as the number of channels of `x`. This results in heap out of bounds reads when the buffers backing these tensors are indexed past their boundary. If the tensors are empty, the validation mentioned in the above paragraph would also trigger and prevent the undefined behavior. 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.	2021-05-14	4.6	CVE-2021-29583 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. TFLite's convolution code(https://github.com/tensorflow/tensorflow/blob/09c73bca7d648e961dd05898292d91a8322a9d45/tensorflow/lite/kernels/conv.cc) has multiple division where the divisor is controlled by the user and not checked to be non-zero. 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.	2021-05-14	4.6	CVE-2021-29594 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `BatchToSpaceNd` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/b5ed552fe55895aee8bd8b191f744a069957d18d/tensorflow/lite/kernels/batch_to_space_nd.cc#L81-L82). An attacker can craft a model such that one dimension of the `block` input is 0. Hence, the corresponding value in `block_shape` is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow	2021-05-14	4.6	CVE-2021-29593 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.			NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The fix for CVE-2020-15209(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15209) missed the case when the target shape of `Reshape` operator is given by the elements of a 1-D tensor. As such, the fix for the vulnerability(https://github.com/tensorflow/tensorflow/blob/9c1dc920d8ffb4893d6c9d27d1f039607b326743/tensorflow/lite/core/subgraph.cc#L1062-L1074) allowed passing a null-buffer-backed tensor with a 1D shape. 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.	2021-05-14	4.6	CVE-2021-29592 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. TFlite graphs must not have loops between nodes. However, this condition was not checked and an attacker could craft models that would result in infinite loop during evaluation. In certain cases, the infinite loop would be replaced by stack overflow due to too many recursive calls. For example, the `While`	2021-05-14	4.6	CVE-2021-29591

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/106d8f4fb89335a2c52d7c895b7a7485465ca8d9/tensorflow/lite/kernels/while.cc) could be tricked into a scneario where both the body and the loop subgraphs are the same. Evaluating one of the subgraphs means calling the `Eval` function for the other and this quickly exhaust all stack space. 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. Please consult our security guide(https://github.com/tensorflow/tensorflow/blob/master/SECURITY.md) for more information regarding the security model and how to contact us with issues and questions.			CONFIRM MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Optimized pooling implementations in TFLite fail to check that the stride arguments are not 0 before calling `ComputePaddingHeightWidth`(https://github.com/tensorflow/tensorflow/blob/3f24ccd932546416ec906a02ddd183b48a1d2c83/tensorflow/lite/kernels/pooling.cc#L90). Since users can craft special models which will have `params->stride_{height,width}` be zero, this will result in a division by zero. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2,	2021-05-14	4.6	CVE-2021-29586 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.			NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The reference implementation of the `GatherNd` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/reference/reference_ops.h#L966). An attacker can craft a model such that `params` input would be an empty tensor. In turn, `params_shape.Dims(.)` would be zero, in at least one dimension. 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.	2021-05-14	4.6	CVE-2021-29589 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The optimized implementation of the `TransposeConv` TFLite operator is [vulnerable to a division by zero error](https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/optimized/optimized_ops.h#L5221-L5222). An attacker can craft a model	2021-05-14	4.6	CVE-2021-29588

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	such that `stride_{h,w}` values are 0. Code calling this function must validate these arguments. 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.			MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The `Prepare` step of the `SpaceToDepth` TFLite operator does not check for 0 before division(https://github.com/tensorflow/tensorflow/blob/5f7975d09eac0f10ed8a17dbb6f5964977725adc/tensorflow/lite/kernels/space_to_depth.cc#L63-L67). An attacker can craft a model such that `params->block_size` would be zero. 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.	2021-05-14	4.6	CVE-2021-29587 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `EmbeddingLookup` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/e4b29809543b25	2021-05-14	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	0bc9b19678ec4776299dd569ba/tensorflow/lite/kernels/embedding_lookup.cc#L73-L74). An attacker can craft a model such that the first dimension of the `value` input is 0. 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.			29596 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in Eigen implementation of `tf.raw_ops.BandedTriangularSolve`. The implementation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/linalg/banded_triangular_solve_op.cc#L269-L278) calls `ValidateInputTensors` for input validation but fails to validate that the two tensors are not empty. Furthermore, since `OP_REQUIRES` macro only stops execution of current function after setting `ctx->status()` to a non-OK value, callers of helper functions that use `OP_REQUIRES` must check value of `ctx->status()` before continuing. This doesn't happen in this op's implementation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/lina	2021-05-14	4.6	CVE-2021-29612 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lg/banded_triangular_solve_op.cc#L219), hence the validation that is present is also not effective. 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.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite computation for size of output after padding, `ComputeOutSize`(https://github.com/tensorflow/tensorflow/blob/0c9692ae7b1671c983569e5d3de5565843d500cf/tensorflow/lite/kernels/padding.h#L43-L55), does not check that the `stride` argument is not 0 before doing the division. Users can craft special models such that `ComputeOutSize` is called with `stride` set to 0. 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.	2021-05-14	4.6	CVE-2021-29585 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `DepthToSpace` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b2	2021-05-14	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/depth_to_space.cc#L63-L69). An attacker can craft a model such that `params->block_size` is 0. 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.			29595 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB read on heap in the TFLite implementation of `Split_V`(https://github.com/tensorflow/tensorflow/blob/c59c37e7b2d563967da813fa50fe20b21f4da683/tensorflow/lite/kernels/split_v.cc#L99). If `axis_value` is not a value between 0 and `NumDimensions(input)`, then the `SizeOfDimension` function(https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39cc65ab/tensorflow/lite/kernels/kernel_util.h#L148-L150) will access data outside the bounds of the tensor shape array. 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.	2021-05-14	4.6	CVE-2021-29606 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `SpaceToBatchNd` TFLite operator is [vulnerable to a division by zero error](https://github.com/tensorflow/tensorflow/blob/412c7d9bb8f8a762c5b266c9e73bfa165f29aac8/tensorflow/lite/kernels/space_to_batch_nd.cc#L82-L83). An attacker can craft a model such that one dimension of the `block` input is 0. Hence, the corresponding value in `block_shape` is 0. 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.	2021-05-14	4.6	CVE-2021-29597 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `SVDF` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/7f283ff806b2031f407db64c4d3edcda8fb9f9f5/tensorflow/lite/kernels/svdf.cc#L99-L102). An attacker can craft a model such that `params->rank` would be 0. 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.	2021-05-14	4.6	CVE-2021-29598 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `Split` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/e2752089ef7ce9bcf3db0ec618ebd23ea119d0c7/tensorflow/lite/kernels/split.cc#L63-L65). An attacker can craft a model such that `num_splits` would be 0. 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.	2021-05-14	4.6	CVE-2021-29599 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `OneHot` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/f61c57bd425878be108ec787f4d96390579fb83e/tensorflow/lite/kernels/one_hot.cc#L68-L72). An attacker can craft a model such that at least one of the dimensions of `indices` would be 0. In turn, the `prefix_dim_size`	2021-05-14	4.6	CVE-2021-29600 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	value would become 0. 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.			NFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB write on heap in the TFLite implementation of `ArgMin`/`ArgMax`(https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39cc65ab/tensorflow/lite/kernels/arg_min_max.cc#L52-L59). If `axis_value` is not a value between 0 and `NumDimensions(input)`, then the condition in the `if` is never true, so code writes past the last valid element of `output_dims->data`. 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.	2021-05-14	4.6	CVE-2021-29603 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data. The	2021-05-14	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/sparse_sparse_binary_op_shared.cc) has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. 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.			29607 MISC MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.RaggedTensorToTensor`, an attacker can exploit an undefined behavior if input arguments are empty. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L356-L360) only checks that one of the tensors is not empty, but does not check for the other ones. There are multiple `DCHECK` validations to prevent heap OOB, but these are	2021-05-14	4.6	CVE-2021-29608 MISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	no-op in release builds, hence they don't prevent anything. The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits 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.			CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/sparse_add_op.cc) has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. 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	2021-05-14	4.6	CVE-2021-29609 MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TensorFlow 2.1.4, as these are also affected and still in supported range.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalAvgPoolGrad` is vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/dcba796a28364d6d7f003f6fe733d82726dda713/tensorflow/core/kernels/fractional_avg_pool_op.cc#L216) fails to validate that the pooling sequence arguments have enough elements as required by the `out_backprop` tensor shape. 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.	2021-05-14	4.6	CVE-2021-29578 MISC CONFIRM
hexagon -- intergraph_g\!nius	Hexagon G!nius Auskunftsportal before 5.0.0.0 allows SQL injection via the GiPWorkflow/Service/DownloadPublicFile id parameter.	2021-05-14	5	CVE-2021-32051 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CMISC MISC
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 199235.	2021-05-14	4.3	CVE-2021-20564 XFCONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a privileged user to inject inject malicious data using a specially crafted HTTP request due to improper input validation.	2021-05-14	4	CVE-2020-481

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				1 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 199236.	2021-05-14	5	CVE-2021-20565 XF CONFIRM
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 could allow an attacker to obtain sensitive information due to accepting body parameters in a query. IBM X-Force ID: 192642.	2021-05-14	5	CVE-2020-498

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				5 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could disclose sensitive information due an overly permissive cross-domain policy. IBM X-Force ID: 196334.	2021-05-14	5	CVE-2021-20429 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196001.	2021-05-14	5	CVE-2021-203

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				93 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-05-14	4.3	CVE-2021-20392 CONFIRM XF
imagemagick -- imagemagick	In ImageMagick versions before 7.0.9-0, there are outside the range of representable values of type 'float' at MagickCore/quantize.c.	2021-05-14	4.3	CVE-2020-277

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				69 MISC
kaspersky -- password_manager	Password generator feature in Kaspersky Password Manager was not completely cryptographically strong and potentially allowed an attacker to predict generated passwords in some cases. An attacker would need to know some additional information (for example, time of password generation).	2021-05-14	5	CVE-2020-27020 MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-18	4	CVE-2020-20222 MISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CFULLDISC
mikrotik -- routeros	Mikrotik RouterOs stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/diskd process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.	2021-05-18	4	CVE-2020-20227 MISC CFULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20237 MISC MISC FULL DISC
mikrotik -- routeros	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20236 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CMISC FULL DISC
mikrotik -- routeros	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the log process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20245 MISC FULL DISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the mactel process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20246 MISC FULL DISC MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from an assertion failure vulnerability in the btest process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	2021-05-18	4	CVE-2020-20214 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM FULLDISC
mikrotik -- routeros	Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/bfd process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-18	4	CVE-2020-20220 CONFIRM FULLDISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mooveagency -- redirect_404_to_parent	The settings page of the Redirect 404 to parent WordPress plugin before 1.3.1 did not properly sanitise the tab parameter before outputting it back, leading to a reflected Cross-Site Scripting issue	2021-05-14	4.3	CVE-2021-24286 CONFIRM
mooveagency -- select_all_categories_and_taxonomies\,_change_checkbox_to_radio_buttons	The settings page of the Select All Categories and Taxonomies, Change Checkbox to Radio Buttons WordPress plugin before 1.3.2 did not properly sanitise the tab parameter before outputting it back, leading to a reflected Cross-Site Scripting issue	2021-05-14	4.3	CVE-2021-24287 CONFIRM
moxa -- nport_ia5150a_firmware	By exploiting a vulnerability in NPort IA5150A/IA5250A Series before version 1.5, a user with “Read Only” privilege level can send	2021-	4	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requests via the web console to have the device's configuration changed.	05-14		2020-27149 MISC MISC
moxa -- nport_ia5150a_firmware	Cleartext transmission of sensitive information via Moxa Service in NPort IA5000A series serial devices. Successfully exploiting the vulnerability could enable attackers to read authentication data, device configuration, and other sensitive data transmitted over Moxa Service.	2021-05-14	5	CVE-2020-27185 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
querysol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the import_from_debug AJAX action to inject PHP objects.	2021-05-14	6.5	CVE-2021-24280 CONFIRM MISC
querysol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the various AJAX actions in the plugin to do a variety of things. For example, an attacker could use wpcf7r_reset_settings to reset the plugin's settings, wpcf7r_add_action to add actions to a form, and more.	2021-05-14	6.5	CVE-2021-24282 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
querysol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, unauthenticated users can use the wpcf7r_get_nonce AJAX action to retrieve a valid nonce for any WordPress action/function.	2021-05-14	5	CVE-2021-24278 MISC CONFIRM
querysol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, low level users, such as subscribers, could use the import_from_debug AJAX action to install any plugin from the WordPress repository.	2021-05-14	4	CVE-2021-24279 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM MISC
querysol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the delete_action_post AJAX action to delete any post on a target site.	2021-05-14	4	CVE-2021-24281 MISC CONFIRM
squirrelly -- squirrelly	Squirrelly is a template engine implemented in JavaScript that works out of the box with ExpressJS. Squirrelly mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options remote code execution may be triggered in downstream applications. There is currently no fix for	2021-05-14	6.8	CVE-2021-328

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	these issues as of the publication of this CVE. The latest version of squirrelly is currently 8.0.8. For complete details refer to the referenced GHSL-2021-023.			19 MISC MISC
tp-link -- archer_c1200_firmware	TP-Link Archer C1200 firmware version 1.13 Build 2018/01/24 rel.52299 EU has a XSS vulnerability allowing a remote attacker to execute arbitrary code.	2021-05-14	4.3	CVE-2020-17891 MISC
upx_project -- upx	A heap buffer overflow read was discovered in upx 4.0.0, because the check in p_lx_elf.cpp is not perfect.	2021-05-14	5.8	CVE-2020-24119 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
wp-buy -- conditional_marketing_mailer	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WooCommerce Conditional Marketing Mailer WordPress plugin before 1.5.2, to install any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnerabilities like RCE.	2021-05-14	6.5	CVE-2021-24190 CONFIRM
wp-buy -- visitor_traffic_real_time_statistics	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Visitor Traffic Real Time Statistics WordPress plugin before 2.12, to install any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnerabilities like RCE.	2021-05-14	6.5	CVE-2021-24193 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xmlsoft -- libxml2	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML mixed content, causing a NULL dereference. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be used to crash the application. The highest threat from this vulnerability is to system availability.	2021-05-14	4.3	CVE-2021-3537 MISC FEDORA MLIST

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dedecms -- dedecms	A XSS Vulnerability in /uploads/dede/action_search.php in DedeCMS V5.7 SP2 allows an authenticated user to execute remote arbitrary code via the keyword parameter.	2021-05-15	3.5	CVE-2020-16632 MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The API of `tf.raw_ops.SparseCross` allows combinations which would result in a `CHECK`-failure and denial of service. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/3d782b7d47b1bf2ed32bd4a246d6d6cadc4c903d/tensorflow/core/kernels/sparse_cross_op.cc#L114-L116) is tricked to consider a tensor of type `tstring` which in fact contains integral elements. Fixing the type confusion by preventing mixing `DT_STRING` and `DT_INT64` types solves this issue. 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.	2021-05-14	2.1	CVE-2021-29519 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.CTCGreedyDecoder`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1615440b17b364b875eb06f43d087381f1460a65/tensorflow/core/kernels/ctc_decoder_ops.cc#L37-L50) has a `CHECK_LT` inserted to validate some invariants. When this condition is false, the program aborts, instead of returning a valid error to the user. This abnormal termination can be weaponized in denial of service attacks. 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.	2021-05-14	2.1	CVE-2021-29543 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Specifying a negative dense shape in `tf.raw_ops.SparseCountSparseOutput` results in a segmentation fault being thrown out from the standard library as `std::vector` invariants are broken. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/count_ops.cc#L199-L213) assumes the first element of the dense shape is always positive and uses it to initialize a `BatchedMap<T>` (i.e., `std::vector<absl::flat_hash_map<int64,T>>`(https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/count	2021-05-14	2.1	CVE-2021-29521 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	_ops.cc#L27)) data structure. If the `shape` tensor has more than one element, `num_batches` is the first value in `shape`. Ensuring that the `dense_shape` argument is a valid tensor shape (that is, all elements are non-negative) solves this issue. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3.			NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can access data outside of bounds of heap allocated array in `tf.raw_ops.UnicodeEncode`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/472c1f12ad9063405737679d4f6bd43094e1d36d/tensorflow/core/kernels/unicode_ops.cc) assumes that the `input_value`/`input_splits` pair specify a valid sparse tensor. 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.	2021-05-14	3.6	CVE-2021-29559 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.RaggedTensorToTensor`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b	2021-05-14	3.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	54115c03cece54f6a1977b/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L219-L222) uses the same index to access two arrays in parallel. Since the user controls the shape of the input arguments, an attacker could trigger a heap OOB access when `parent_output_index` is shorter than `row_split`. 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.			29560 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ac328eaa3870491ababc147822cd04e91a790643/tensorflow/core/kernels/requantization_range_op.cc#L49-L50) assumes that the `input_min` and `input_max` tensors have at least one element, as it accesses the first element in two arrays. If the tensors are empty, `.flat<T>()` is an empty object, backed by an empty array. Hence, accesing even the 0th element is a read outside the bounds. 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.	2021-05-14	3.6	CVE-2021-29569 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of	2021-	3.6	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ef0c008ee84bad91ec6725ddc42091e19a30cf0e/tensorflow/core/kernels/maxpooling_op.cc#L1016-L1017) uses the same value to index in two different arrays but there is no guarantee that the sizes are identical. 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.	05-14		2021-29570 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.Dequantize`, an attacker can trigger a read from outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/26003593aa94b1742f34dc22ce88a1e17776a67d/tensorflow/core/kernels/dequantize_op.cc#L106-L131) accesses the `min_range` and `max_range` tensors in parallel but fails to check that they have the same shape. 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.	2021-05-14	3.6	CVE-2021-29582 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementations of the `Minimum` and `Maximum` TFLite operators can be used to read data outside of bounds of heap allocated objects, if any of the two input tensor arguments are empty. This is because the broadcasting implementation(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/reference/maximum_minimum.h#L52-L56) indexes in both tensors with the same index but does not validate that the index is within bounds. 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.	2021-05-14	3.6	CVE-2021-29590 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of concatenation is vulnerable to an integer overflow issue(https://github.com/tensorflow/tensorflow/blob/7b7352a724b690b11bfaae2cd54bc3907daf6285/tensorflow/lite/kernels/concatenation.cc#L70-L76). An attacker can craft a model such that the dimensions of one of the concatenation input overflow the values of `int`. TFLite uses `int` to represent tensor dimensions, whereas TF uses `int64`. Hence, valid TF models can trigger an integer overflow when converted to TFLite format. 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.	2021-05-14	3.6	CVE-2021-29601 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `tf.raw_ops.CTCLoss` allows an attacker to trigger an OOB read from heap. The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits 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.	2021-05-14	3.6	CVE-2021-29613 CONFIRM MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.RaggedTensorToVariant` with arguments specifying an invalid ragged tensor results in a null pointer dereference. The implementation of `RaggedTensorToVariant` operations(https://github.com/tensorflow/tensorflow/blob/904b3926ed1c6c70380d531	2021-05-14	2.1	CVE-2021-295

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3d282d248a776baa1/tensorflow/core/kernels/ragged_tensor_to_variant_op.cc#L39-L40) does not validate that the ragged tensor argument is non-empty. Since `batched_ragged` contains no elements, `batched_ragged.splits` is a null vector, thus `batched_ragged.splits(0)` will result in dereferencing `nullptr`. 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.			16 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can read data outside of bounds of heap allocated buffer in `tf.raw_ops.QuantizeAndDequantizeV3`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/11ff7f80667e6490d7b5174aa6bf5e01886e770f/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L237) does not validate the value of user supplied `axis` attribute before using it to index in the array backing the `input` argument. 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.	2021-05-14	3.6	CVE-2021-29553 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A malicious user could trigger a division by 0 in `Conv3D` implementation. The	2021-	2.1	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/42033603003965bffac51ae171b51801565e002d/tensorflow/core/kernels/conv_ops_3d.cc#L143-L145) does a modulo operation based on user controlled input. Thus, when `filter` has a 0 as the fifth element, this results in a division by 0. Additionally, if the shape of the two tensors is not valid, an Eigen assertion can be triggered, resulting in a program crash. 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.	05-14		2021-29517 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in converting sparse tensors to CSR Sparse matrices. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/800346f2c03a27e182dd4fba48295f65e7790739/tensorflow/core/kernels/sparse/kernels.cc#L66) does a double redirection to access an element of an array allocated on the heap. If the value at `indices(i, 0)` is such that `indices(i, 0) + 1` is outside the bounds of `csr_row_ptr`, this results in writing outside of bounds of heap allocated data. 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.	2021-05-14	2.1	CVE-2021-29545 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The `tf.raw_ops.Conv3DBackprop*` operations fail to validate that the input tensors are not empty. In turn, this would result in a division by 0. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a91bb59769f19146d5a0c20060244378e878f140/tensorflow/core/kernels/conv_grad_ops_3d.cc#L430-L450) does not check that the divisor used in computing the shard size is not zero. Thus, if attacker controls the input sizes, they can trigger a denial of service via a division by zero error. 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.	2021-05-14	2.1	CVE-2021-29522 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.QuantizedConv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/00e9a4d67d76703fa1aee33dac582acf317e0e81/tensorflow/core/kernels/quantized_conv_ops.cc#L257-L259) does a division by a quantity that is controlled by the caller. 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.	2021-05-14	2.1	CVE-2021-29527 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a dereference of a null pointer in `tf.raw_ops.StringNGrams`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op.cc#L67-L74) does not fully validate the `data_splits` argument. This would result in `ngrams_data`(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op.cc#L106-L110) to be a null pointer when the output would be computed to have 0 or negative size. Later writes to the output tensor would then cause a null pointer dereference. 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.	2021-05-14	2.1	CVE-2021-29541 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.ImmutableConst`(https://www.tensorflow.org/api_docs/python/tf/raw_ops/ImmutableConst) with a `dtype` of `tf.resource` or `tf.variant` results in a segfault in the implementation as code assumes that the tensor contents are pure scalars. We have patched the issue in 4f663d4b8f0bec1b48da6fa091a7d29609980fa4 and will release	2021-05-14	2.1	CVE-2021-295

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TensorFlow 2.5.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved. If using `tf.raw_ops.ImmutableConst` in code, you can prevent the segfault by inserting a filter for the `dtype` argument.			39 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a division by zero to occur in `Conv2DBackpropFilter`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv_grad_filter_ops.cc#L513-L522) computes a divisor based on user provided data (i.e., the shape of the tensors given as arguments). If all shapes are empty then `work_unit_size` is 0. Since there is no check for this case before division, this results in a runtime exception, with potential to be abused for a denial of service. 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.	2021-05-14	2.1	CVE-2021-29538 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.SparseConcat`. This is because the	2021-	2.1	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/b432a38fe0e1b4b904a6c222cbce794c39703e87/tensorflow/core/kernels/sparse_concat_op.cc#L76) takes the values specified in `shapes[0]` as dimensions for the output shape. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) uses a `CHECK` operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L212-L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to prevent `CHECK`-failures in the presence of overflows. 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.	05-14		1-29534 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK` failure by passing an empty image to `tf.raw_ops.DrawBoundingBoxes`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/ea34a18dc3f5c8d80a40ccca1404f343b5d55f91/tensorflow/core/kernels/image/draw_bounding_box_op.cc#L148-L165) uses `CHECK_*` assertions instead of `OP_REQUIRES` to validate user controlled inputs. Whereas `OP_REQUIRES` allows returning an error condition back	2021-05-14	2.1	CVE-2021-29533 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to the user, the `CHECK_*` macros result in a crash if the condition is false, similar to `assert`. In this case, `height` is 0 from the `images` input. This results in `max_box_row_clamp` being negative and the assertion being falsified, followed by aborting program execution. 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.			NFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a `CHECK` fail in PNG encoding by providing an empty input tensor as the pixel data. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/kernels/image/encode_png_op.cc#L57-L60) only validates that the total number of pixels in the image does not overflow. Thus, an attacker can send an empty matrix for encoding. However, if the tensor is empty, then the associated buffer is `nullptr`. Hence, when calling `png::WriteImageToBuffer`(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/kernels/image/encode_png_op.cc#L79-L93), the first argument (i.e., `image.flat<T>().data()`) is `NULL`. This then triggers the `CHECK_NOTNULL` in the first line of `png::WriteImageToBuffer`(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/lib/png/png_io.cc#L345-L349). Since `image` is null, this results in `abort` being called after printing the	2021-05-14	2.1	CVE-2021-29531 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stacktrace. Effectively, this allows an attacker to mount a denial of service attack. 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.			
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.QuantizedMul`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55900e961ed4a23b438392024912154a2c2f5e85/tensorflow/core/kernels/quantized_mul_op.cc#L188-L198) does a division by a quantity that is controlled by the caller. 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.	2021-05-14	2.1	CVE-2021-29528 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Passing invalid arguments (e.g., discovered via fuzzing) to `tf.raw_ops.SparseCountSparseOutput` results in segfault. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2,	2021-05-14	2.1	CVE-2021-296

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.			19 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/988087bd83f144af14087fe4fecee2d250d93737/tensorflow/core/kernels/conv_ops.cc#L261-L263) does a division by a quantity that is controlled by the caller. 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.	2021-05-14	2.1	CVE-2021-29526 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.AddManySparseToTensorsMap`. This is because the	2021-	2.1	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/kernels/sparse_tensors_map_ops.cc#L257) takes the values specified in `sparse_shape` as dimensions for the output shape. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) uses a `CHECK` operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L212-L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to prevent `CHECK`-failures in the presence of overflows. 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.	05-14		1-29523 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropFilter`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/496c2630e51c1a478f095b084329acedb253db6b/tensorflow/core/kernels/conv_grad_shape_utils.cc#L130) does a modulus operation where the divisor is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow	2021-05-14	2.1	CVE-2021-29524

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can force accesses outside the bounds of heap allocated arrays by passing in invalid tensor values to `tf.raw_ops.RaggedCross`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/efea03b38fb8d3b81762237dc85e579cc5fc6e87/tensorflow/core/kernels/ragged_cross_op.cc#L456-L487) lacks validation for the user supplied arguments. Each of the above branches call a helper function after accessing array elements via a `*_list[next_*]` pattern, followed by incrementing the `next_*` index. However, as there is no validation that the `next_*` values are in the valid range for the corresponding `*_list` arrays, this results in heap OOB reads. 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.	2021-05-14	3.6	CVE-2021-29532 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow by passing crafted inputs to `tf.raw_ops.StringNGrams`. This is because the	2021-	2.1	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op.cc#L171-L185) fails to consider corner cases where input would be split in such a way that the generated tokens should only contain padding elements. If input is such that `num_tokens` is 0, then, for `data_start_index=0` (when left padding is present), the marked line would result in reading `data[-1]`. 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.	05-14		1-29542 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Passing a complex argument to `tf.transpose` at the same time as passing `conjugate=True` argument results in a crash. 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.	2021-05-14	2.1	CVE-2021-29618 MISC CONFIRM MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CMISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the implementation of `tf.raw_ops.RFFT`. Eigen code operating on an empty matrix can trigger on an assertion and will cause program termination. 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.	2021-05-14	2.1	CVE-2021-29563 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.EditDistance`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/79865b542f9ffdc9caeb255631f7c56f1d4b6517/tensorflow/core/kernels/edit_distance_op.cc#L103-L159) has incomplete validation of the input parameters. The fix will be included in TensorFlow	2021-05-14	2.1	CVE-2021-29564

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a segfault and denial of service via accessing data outside of bounds in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0bbbeb414dc55553d3ae7f/tensorflow/core/kernels/quantized_batch_norm_op.cc#L176-L189) assumes the inputs are not empty. If any of these inputs is empty, `.flat<T>()` is an empty buffer, so accessing the element at index 0 is accessing data outside of bounds. 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.	2021-05-14	2.1	CVE-2021-29547 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0	2021-05-14	2.1	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bbbeb414dc55553d3ae7f/tensorflow/core/kernels/quantized_batch_norm_op.cc) does not validate all constraints specified in the op's contract(https://www.tensorflow.org/api_docs/python/tf/raw_ops/QuantizedBatchNormWithGlobalNormalization). 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.			29548 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/kernels/quantized_add_op.cc#L289-L295) computes a modulo operation without validating that the divisor is not zero. Since `vector_num_elements` is determined based on input shapes(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/kernels/quantized_add_op.cc#L522-L544), a user can trigger scenarios where this quantity is 0. 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.	2021-05-14	2.1	CVE-2021-29549 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.FractionalAvgPool`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_avg_pool_op.cc#L85-L89) computes a divisor quantity by dividing two user controlled values. The user controls the values of `input_size[i]` and `pooling_ratio_[i]` (via the `value.shape()` and `pooling_ratio` arguments). If the value in `input_size[i]` is smaller than the `pooling_ratio_[i]`, then the floor operation results in `output_size[i]` being 0. The `DCHECK_GT` line is a no-op outside of debug mode, so in released versions of TF this does not trigger. Later, these computed values are used as arguments(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_avg_pool_op.cc#L96-L99) to `GeneratePoolingSequence`(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_pool_common.cc#L100-L108). There, the first computation is a division in a modulo operation. Since `output_length` can be 0, this results in runtime crashing. 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.	2021-05-14	2.1	CVE-2021-29550 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `MatrixTriangularSolve`(https://github.com/tensorflow/tensorflow/blob/8cae746d8449c7dda5298327353d68613f16e798/tensorflow/core/kernels/linalg/matrix_triangular_solve_op_impl.h#L160-L240) fails to terminate kernel execution if one validation condition fails. 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.	2021-05-14	2.1	CVE-2021-29551 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by controlling the values of `num_segments` tensor argument for `UnsortedSegmentJoin`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a2a607db15c7cd01d754d37e5448d72a13491bdb/tensorflow/core/kernels/unsorted_segment_join_op.cc#L92-L93) assumes that the `num_segments` tensor is a valid scalar. Since the tensor is empty the `CHECK` involved in `.scalar<T>()()` that checks that the number of elements is exactly 1 will be invalidated and this would result in process termination. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on	2021-05-14	2.1	CVE-2021-29552 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.DenseCountSparseOutput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/efff014f3b2d8ef6141da30c806faf141297eca1/tensorflow/core/kernels/count_ops.cc#L123-L127) computes a divisor value from user data but does not check that the result is 0 before doing the division. Since `data` is given by the `values` argument, `num_batch_elements` is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, and TensorFlow 2.3.3, as these are also affected.	2021-05-14	2.1	CVE-2021-29554 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.FusedBatchNorm`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/828f346274841fa7505f7020e88ca36c22e557ab/tensorflow/core/kernels/fused_batch_norm_op.cc#L295-L297) performs a division based on the last dimension of the `x` tensor. Since this is controlled by the user, an attacker can trigger a denial of service. The fix will be	2021-05-14	2.1	CVE-2021-29555 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			NFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.Reverse`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/36229ea9e9451dac14a8b1f4711c435a1d84a594/tensorflow/core/kernels/reverse_op.cc#L75-L76) performs a division based on the first dimension of the tensor argument. 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.	2021-05-14	2.1	CVE-2021-29556 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.SparseMatMul`. The division by 0 occurs deep in Eigen code because the `b` tensor is empty. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on	2021-05-14	2.1	CVE-2021-295

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			57 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via `CHECK`-fail in `tf.strings.substr` with invalid arguments. 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.	2021-05-14	2.1	CVE-2021-29617 MISC CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the implementation of `tf.raw_ops.IRFFT`. 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.	2021-05-14	2.1	CVE-2021-29562 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from `tf.raw_ops.LoadAndRemapMatrix`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cece54f6a1977b/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L219-L222) assumes that the `ckpt_path` is always a valid scalar. However, an attacker can send any other tensor as the first argument of `LoadAndRemapMatrix`. This would cause the rank `CHECK` in `scalar<T>()()` to trigger and terminate the process. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this	2021-05-14	2.1	CVE-2021-29561 MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			NFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.SparseDenseCwiseMul`, an attacker can trigger denial of service via `CHECK`-fails or accesses to outside the bounds of heap allocated data. Since the implementation(https://github.com/tensorflow/tensorflow/blob/38178a2f7a681a7835bb0912702a134bfe3b4d84/tensorflow/core/kernels/sparse_dense_binary_op_shared.cc#L68-L80) only validates the rank of the input arguments but no constraints between dimensions(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SparseDenseCwiseMul), an attacker can abuse them to trigger internal `CHECK` assertions (and cause program termination, denial of service) or to write to memory outside of bounds of heap allocated tensor buffers. 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.	2021-05-14	2.1	CVE-2021-29567 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in caused by an integer overflow in constructing a new tensor shape. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/0908c2f2397c099338b901b067f6495a5b96760b/tensorflow/core/kernels/sparse_split_op.cc#L66-L70)	2021-05-14	2.1	CVE-2021-295

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	builds a dense shape without checking that the dimensions would not result in overflow. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) uses a `CHECK` operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L212-L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to prevent `CHECK`-failures in the presence of overflows. 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.			84 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `ParseAttrValue`(https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fc9aa74ed79595/tensorflow/core/framework/attr_value_util.cc#L397-L453) can be tricked into stack overflow due to recursion by giving in a specially crafted input. 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.	2021-05-14	2.1	CVE-2021-29615 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseReshape` results in a denial of service based on a `CHECK`-failure. The implementation(https://github.com/tensorflow/tensorflow/blob/e87b51ce05c3eb172065a6ea5f48415854223285/tensorflow/core/kernels/sparse_reshape_op.cc#L40) has no validation that the input arguments specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are the only affected versions.	2021-05-14	2.1	CVE-2021-29611 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite code for allocating `TFLiteIntArray`s is vulnerable to an integer overflow issue(https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cdfa/tensorflow/lite/c/common.c#L24-L27). An attacker can craft a model such that the `size` multiplier is so large that the return value overflows the `int` datatype and becomes negative. In turn, this results in invalid value being given to	2021-05-14	2.1	CVE-2021-29605

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`malloc`(https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cdfa/tensorflow/lite/c/common.c#L47-L52). In this case, `ret->size` would dereference an invalid 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.			CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.SparseFillEmptyRows`. This is because of missing validation(https://github.com/tensorflow/tensorflow/blob/fdc82089d206e281c628a93771336bf87863d5e8/tensorflow/core/kernels/sparse_fill_empty_rows_op.cc#L230-L231) that was covered under a `TODO`. If the `dense_shape` tensor is empty, then `dense_shape_t.vec<>()` would cause a null pointer dereference in the implementation of the op. 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.	2021-05-14	2.1	CVE-2021-29565 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `DepthwiseConv` TFLite operator is vulnerable to a division by zero	2021-	2.1	CVE-202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	error(https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e833bc8/tensorflow/lite/kernels/depthwise_conv.cc#L287-L288). An attacker can craft a model such that `input`'s fourth dimension would be 0. 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.	05-14		1-29602 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of hashtable lookup is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e833bc8/tensorflow/lite/kernels/hashtable_lookup.cc#L114-L115) An attacker can craft a model such that `values`'s first dimension would be 0. 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.	2021-05-14	2.1	CVE-2021-29604 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.CTCBeamSearchDecoder`, an attacker can trigger denial of service via segmentation faults. The implementation(https://github.com/tensorflow/tensorflow/blob/a74768f8e4efbda4def9f16ee7e13cf3922ac5f7/tensorflow/core/kernels/ctc_decoder_ops.cc#L68-L79) fails to detect cases when the input tensor is empty and proceeds to read data from a null buffer. 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.	2021-05-14	2.1	CVE-2021-29581 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalMaxPoolGrad` triggers an undefined behavior if one of the input tensors is empty. The code is also vulnerable to a denial of service attack as a `CHECK` condition becomes false and aborts the process. The implementation(https://github.com/tensorflow/tensorflow/blob/169054888d50ce488dfde9ca55d91d6325efbd5b/tensorflow/core/kernels/fractional_max_pool_op.cc#L215) fails to validate that input and output tensors are not empty and are of the same rank. Each of these unchecked assumptions is responsible for the above issues. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow	2021-05-14	2.1	CVE-2021-29580 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.ReverseSequence` allows for stack overflow and/or `CHECK`-fail based denial of service. The implementation(https://github.com/tensorflow/tensorflow/blob/5b3b071975e01f0d250c928b2a8f901cd53b90a7/tensorflow/core/kernels/reverse_sequence_op.cc#L114-L118) fails to validate that `seq_dim` and `batch_dim` arguments are valid. Negative values for `seq_dim` can result in stack overflow or `CHECK`-failure, depending on the version of Eigen code used to implement the operation. Similar behavior can be exhibited by invalid values of `batch_dim`. 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.	2021-05-14	2.1	CVE-2021-29575 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` is vulnerable to a division by 0. The implementation(https://github.com/tensorflow/tensorflow/blob/279bab6efa22752a2827621b7edb56a730233bd8/tensorflow/core/kernels/maxpooling_op.cc#L1033-L1034) fails to validate that the batch dimension of the tensor is non-zero, before dividing by	2021-05-14	2.1	CVE-2021-29573

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this quantity. 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.			CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.SdcaOptimizer` triggers undefined behavior due to dereferencing a null pointer. The implementation(https://github.com/tensorflow/tensorflow/blob/60a45c8b6192a4699f2e2709a2645a751d435cc3/tensorflow/core/kernels/sdca_internal.cc) does not validate that the user supplied arguments satisfy all constraints expected by the op(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SdcaOptimizer). 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.	2021-05-14	2.1	CVE-2021-29572 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.QuantizeAndDequantizeV4Grad`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/95078c145b5a7a43ee0	2021-05-14	2.1	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	46144005f733092756ab5/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L162-L163) does not validate the rank of the `input_*` tensors. In turn, this results in the tensors being passes as they are to `QuantizeAndDequantizePerChannelGradientImpl`(https://github.com/tensorflow/tensorflow/blob/95078c145b5a7a43ee046144005f733092756ab5/tensorflow/core/kernels/quantize_and_dequantize_op.h#L295-L306). However, the `vec<T>` method, requires the rank to 1 and triggers a `CHECK` failure otherwise. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 as this is the only other affected version.			29544 MISC CONFIRM
haml-coffee_project -- haml-coffee	haml-coffee is a JavaScript templating solution. haml-coffee mixes pure template data with engine configuration options through the Express render API. More specifically, haml-coffee supports overriding a series of HTML helper functions through its configuration options. A vulnerable application that passes user controlled request objects to the haml-coffee template engine may introduce RCE vulnerabilities. Additionally control over the escapeHtml parameter through template configuration pollution ensures that haml-coffee would not sanitize template inputs that may result in reflected Cross Site Scripting attacks against downstream applications. There is currently no fix for these issues as of the publication of this CVE. The latest version of haml-coffee is currently 1.14.1. For complete details refer to the referenced GHSL-2021-025.	2021-05-14	3.5	CVE-2021-32818 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 195999.	2021-05-14	2.1	CVE-2021-20391 XFCONFIRM
laobancms -- laobancms	Cross Site Scripting (XSS) in LAOBANCMS v2.0 allows remote attackers to execute arbitrary code by injecting commands into the "Homepage Introduction" field of component "admin/info.php?shuyu".	2021-05-14	3.5	CVE-2020-18167 MISC
pickplugins -- accordion	The tab GET parameter of the settings page is not sanitised or escaped when being output back in an HTML attribute, leading to a reflected XSS issue.	2021-	3.5	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		05-14		2021-24283 CONFIRM
wpuslugi -- rss_for_yandex_turbo	The RSS for Yandex Turbo WordPress plugin before 1.30 did not properly sanitise the user inputs from its Ð¡Ñ‡ÐµÑ‚Ñ‡Ð¸ÐºÐ¸ settings tab before outputting them back in the page, leading to authenticated stored Cross-Site Scripting issues	2021-05-14	3.5	CVE-2021-24277 CONFIRM
yfcmf -- yfcmf	In YFCMF v2.3.1, there is a stored XSS vulnerability in the comments section of the news page.	2021-05-14	3.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				23689 MISC