Data for SBOM Document ID: 78389675-0358-46e5-81c7-04186dbfb8a8

Metadata

Key	Value
Timestamp	2023-09-06T12:49:53+00:00

Components

Name	Version
tests/pulsar-client-all-shade-test/pom.xml	
tests/pom.xml	
pulsar-io/jdbc/mariadb/pom.xml	
pulsar-client-admin-shaded/pom.xml	
bouncy-castle/bc/pom.xml	
tests/pulsar-client-shade-test/pom.xml	
pulsar-io/alluxio/pom.xml	
pulsar-io/common/pom.xml	
pulsar-package-management/bookkeeper-storage/pom.xml	
pulsar-io/jdbc/clickhouse/pom.xml	
pulsar-client-1x-base/pulsar-client-1x/pom.xml	
pulsar-io/aerospike/pom.xml	
docker/pom.xml	
pulsar-config-validation/pom.xml	
pulsar-transaction/pom.xml	
pulsar-io/hdfs3/pom.xml	
distribution/offloaders/pom.xml	
pulsar-package-management/filesystem-storage/pom.xml	
pulsar-functions/proto/pom.xml	
pulsar-common/pom.xml	
tiered-storage/file-system/pom.xml	
pulsar-functions/api-java/pom.xml	
pulsar-io/jdbc/postgres/pom.xml	
buildtools/pom.xml	
managed-ledger/pom.xml	

pulsar-function-go/go.mod	
pulsar-client-tools-api/pom.xml	
pulsar-sql/presto-pulsar-plugin/pom.xml	
pulsar-functions/java-examples-builtin/pom.xml	
bouncy-castle/pom.xml	
pulsar-client-api/pom.xml	
pulsar-functions/runtime/pom.xml	
pulsar-client-auth-sasl/pom.xml	
pulsar-io/debezium/oracle/pom.xml	
pulsar-client-tools/pom.xml	
pulsar-proxy/pom.xml	
tests/docker-images/java-test-plugins/pom.xml	
pulsar-io/debezium/postgres/pom.xml	
pulsar-io/solr/pom.xml	
pulsar-io/pom.xml	
pulsar-functions/utils/pom.xml	
pulsar-io/debezium/pom.xml	
pulsar-broker-common/pom.xml	
tests/integration/pom.xml	
pulsar-io/file/pom.xml	
pulsar-package-management/pom.xml	
pulsar-transaction/common/pom.xml	
pulsar-functions/worker/pom.xml	
pulsar-io/debezium/mongodb/pom.xml	
pulsar-io/core/pom.xml	
pulsar-io/jdbc/core/pom.xml	
pulsar-client-admin/pom.xml	
tests/docker-images/latest-version-image/pom.xml	
pulsar-functions/localrun-shaded/pom.xml	
pulsar-metadata/pom.xml	
pulsar-io/mongo/pom.xml	
pulsar-io/kinesis/pom.xml	
pulsar-client-messagecrypto-bc/pom.xml	

pulsar-functions/runtime-all/pom.xml	
pulsar-functions/java-examples/pom.xml	
bouncy-castle/bcfips-include-test/pom.xml	
pulsar-function-go/examples/go.mod	
pulsar-io/kafka-connect-adaptor-nar/pom.xml	
pulsar-sql/presto-distribution/pom.xml	
pulsar-functions/pom.xml	
pulsar-io/dynamodb/pom.xml	
testmocks/pom.xml	
bouncy-castle/bcfips/pom.xml	
pulsar-io/cassandra/pom.xml	
docker/pulsar-all/pom.xml	
pulsar-io/flume/pom.xml	
pulsar-websocket/pom.xml	
pulsar-client-1x-base/pom.xml	
pulsar-io/elastic-search/pom.xml	
pom.xml	
pulsar-io/rabbitmq/pom.xml	
tiered-storage/pom.xml	
pulsar-io/debezium/mysql/pom.xml	
pulsar-io/debezium/mssql/pom.xml	
pulsar-functions/instance/pom.xml	
pulsar-io/redis/pom.xml	
distribution/server/pom.xml	
pulsar-io/batch-discovery-triggerers/pom.xml	
pulsar-io/influxdb/pom.xml	
pulsar-package-management/core/pom.xml	
pulsar-client-1x-base/pulsar-client-2x-shaded/pom.xml	
pulsar-functions/secrets/pom.xml	
pulsar-client-all/pom.xml	
tests/pulsar-client-admin-shade-test/pom.xml	
distribution/pom.xml	
pulsar-testclient/pom.xml	

pulsar-io/kafka-connect-adaptor/pom.xml	
tests/bc_2_0_1/pom.xml	
pulsar-client-tools-customcommand-example/pom.xml	
pulsar-docs-tools/pom.xml	
tests/bc_2_6_0/pom.xml	
structured-event-log/pom.xml	
pulsar-io/jdbc/sqlite/pom.xml	
pulsar-broker-auth-oidc/pom.xml	
pulsar-broker/pom.xml	
pulsar-client-admin-api/pom.xml	
pulsar-io/batch-data-generator/pom.xml	
pulsar-io/twitter/pom.xml	
pulsar-io/canal/pom.xml	
distribution/shell/pom.xml	
pulsar-io/jdbc/openmldb/pom.xml	
pulsar-io/netty/pom.xml	
tests/docker-images/pom.xml	
pulsar-io/nsq/pom.xml	
pulsar-io/hdfs2/pom.xml	
tests/docker-images/java-test-image/pom.xml	
distribution/io/pom.xml	
docker/pulsar/pom.xml	
jclouds-shaded/pom.xml	
pulsar-cli-utils/pom.xml	
pulsar-io/aws/pom.xml	
pulsar-io/http/pom.xml	
pulsar-transaction/coordinator/pom.xml	
tiered-storage/jcloud/pom.xml	
pulsar-io/debezium/core/pom.xml	
pulsar-io/data-generator/pom.xml	
pulsar-io/hbase/pom.xml	
pulsar-client-tools-test/pom.xml	
pulsar-client/pom.xml	

pulsar-client-auth-athenz/pom.xml	
pulsar-io/jdbc/pom.xml	
pulsar-functions/localrun/pom.xml	
pulsar-sql/pom.xml	
tests/docker-images/java-test-functions/pom.xml	
pulsar-client-shaded/pom.xml	
tests/bc_2_0_0/pom.xml	
pulsar-sql/presto-pulsar/pom.xml	
pulsar-io/docs/pom.xml	
pulsar-broker-auth-sasl/pom.xml	
pulsar-broker-auth-athenz/pom.xml	
pulsar-io/kafka/pom.xml	
cloud.google.com/go/bigquery	1.8.0
cloud.google.com/go/datastore	1.1.0
cloud.google.com/go/firestore	1.1.0
cloud.google.com/go/pubsub	1.3.1
cloud.google.com/go/storage	1.10.0
cloud.google.com/go	0.81.0
dmitri.shuralyov.com/gpu/mtl	0.0.0-20190408044501-666a987793e9
github.com/99designs/keyring	1.1.6
github.com/alecthomas/template	0.0.0-20190718012654-fb15b899a751
github.com/alecthomas/units	0.0.0-20190924025748-f65c72e2690d
github.com/antihax/optional	1.0.0
github.com/apache/pulsar-client-go/oauth2	0.0.0-20220120090717-25e59572242e
github.com/apache/pulsar-client-go	0.8.1
github.com/ardielle/ardielle-go	1.5.2
github.com/ardielle/ardielle-tools	1.5.4
github.com/armon/circbuf	0.0.0-20150827004946-bbbad097214e
github.com/armon/go-metrics	0.0.0-20180917152333-f0300d1749da
github.com/armon/go-radix	0.0.0-20180808171621-7fddfc383310
github.com/AthenZ/athenz	1.10.39
github.com/aws/aws-sdk-go	1.32.6
github.com/beefsack/go-rate	0.0.0-20220214233405-116f4ca011a0

github.com/beorn7/perks	1.0.1
github.com/bgentry/speakeasy	0.1.0
github.com/bketelsen/crypt	0.0.4
github.com/bmizerany/perks	0.0.0-20141205001514-d9a9656a3a4b
github.com/BurntSushi/toml	0.3.1
github.com/BurntSushi/xgb	0.0.0-20160522181843-27f122750802
github.com/census-instrumentation/opencensus-proto	0.2.1
github.com/cespare/xxhash/v2	2.1.2
github.com/chzyer/logex	1.1.10
github.com/chzyer/readline	0.0.0-20180603132655-2972be24d48e
github.com/chzyer/test	0.0.0-20180213035817-a1ea475d72b1
github.com/client9/misspell	0.3.4
github.com/cncf/udpa/go	0.0.0-20201120205902-5459f2c99403
github.com/coreos/go-semver	0.3.0
github.com/coreos/go-systemd/v22	22.3.2
github.com/cpuguy83/go-md2man/v2	2.0.0
github.com/danieljoos/wincred	1.0.2
github.com/DataDog/zstd	1.5.0
github.com/davecgh/go-spew	1.1.1
github.com/dimfeld/httptreemux	5.0.1+incompatible
github.com/dvsekhvalnov/jose2go	0.0.0-20200901110807-248326c1351b
github.com/envoyproxy/go-control-plane	0.9.9-0.20210217033140-668b12f5399d
github.com/envoyproxy/protoc-gen-validate	0.1.0
github.com/fatih/color	1.7.0
github.com/fsnotify/fsnotify	1.4.9
github.com/ghodss/yaml	1.0.0
github.com/go-gl/glfw/v3.3/glfw	0.0.0-20200222043503-6f7a984d4dc4
github.com/go-gl/glfw	0.0.0-20190409004039-e6da0acd62b1
github.com/go-kit/kit	0.9.0
github.com/go-kit/log	0.1.0
github.com/go-logfmt/logfmt	0.5.0
github.com/go-sql-driver/mysql	1.5.0
github.com/go-stack/stack	1.8.0

github.com/godbus/dbus/v5	5.0.4
github.com/godbus/dbus	0.0.0-20190726142602-4481cbc300e2
github.com/gogo/protobuf	1.3.2
github.com/golang-jwt/jwt	3.2.2+incompatible
github.com/golang/glog	0.0.0-20160126235308-23def4e6c14b
github.com/golang/groupcache	0.0.0-20200121045136-8c9f03a8e57e
github.com/golang/mock	1.5.0
github.com/golang/protobuf	1.5.2
github.com/golang/snappy	0.0.1
github.com/google/btree	1.0.0
github.com/google/go-cmp	0.5.5
github.com/google/gofuzz	1.0.0
github.com/google/martian/v3	3.1.0
github.com/google/martian	2.1.0+incompatible
github.com/google/pprof	0.0.0-20210226084205-cbba55b83ad5
github.com/google/renameio	0.1.0
github.com/google/uuid	1.1.2
github.com/googleapis/gax-go/v2	2.0.5
github.com/gopherjs/gopherjs	0.0.0-20181017120253-0766667cb4d1
github.com/gorilla/mux	1.7.4
github.com/grpc-ecosystem/grpc-gateway	1.16.0
github.com/gsterjov/go-libsecret	0.0.0-20161001094733-a6f4afe4910c
github.com/hashicorp/consul/api	1.1.0
github.com/hashicorp/consul/sdk	0.1.1
github.com/hashicorp/errwrap	1.0.0
github.com/hashicorp/go-cleanhttp	0.5.1
github.com/hashicorp/go-immutable-radix	1.0.0
github.com/hashicorp/go-msgpack	0.5.3
github.com/hashicorp/go-multierror	1.0.0
github.com/hashicorp/go-rootcerts	1.0.0
github.com/hashicorp/go-sockaddr	1.0.0
github.com/hashicorp/go-syslog	1.0.0
github.com/hashicorp/go-uuid	1.0.1

github.com/hashicorp/go.net	0.0.1
github.com/hashicorp/golang-lru	0.5.1
github.com/hashicorp/hcl	1.0.0
github.com/hashicorp/logutils	1.0.0
github.com/hashicorp/mdns	1.0.0
github.com/hashicorp/memberlist	0.1.3
github.com/hashicorp/serf	0.8.2
github.com/hpcloud/tail	1.0.0
github.com/ianlancetaylor/demangle	0.0.0-20200824232613-28f6c0f3b639
github.com/inconshreveable/mousetrap	1.0.0
github.com/jawher/mow.cli	1.2.0
github.com/jmespath/go-jmespath	0.3.0
github.com/jpillora/backoff	1.0.0
github.com/json-iterator/go	1.1.11
github.com/json-iterator/go	1.1.12
github.com/jstemmer/go-junit-report	0.9.1
github.com/jtolds/gls	4.20.0+incompatible
github.com/julienschmidt/httprouter	1.3.0
github.com/keybase/go-keychain	0.0.0-20190712205309-48d3d31d256d
github.com/kisielk/errcheck	1.5.0
github.com/kisielk/gotool	1.0.0
github.com/klauspost/compress	1.10.8
github.com/konsorten/go-windows-terminal-sequences	1.0.3
github.com/kr/fs	0.1.0
github.com/kr/logfmt	0.0.0-20140226030751-b84e30acd515
github.com/kr/pretty	0.2.0
github.com/kr/pty	1.1.1
github.com/kr/text	0.1.0
github.com/linkedin/goavro/v2	2.9.8
github.com/magiconair/properties	1.8.5
github.com/mattn/go-colorable	0.0.9
github.com/mattn/go-isatty	0.0.3
github.com/matttproud/golang_protobuf_extensions	1.0.1

github.com/miekg/dns	1.0.14
github.com/mitchellh/cli	1.0.0
github.com/mitchellh/go-homedir	1.1.0
github.com/mitchellh/go-testing-interface	1.0.0
github.com/mitchellh/gox	0.4.0
github.com/mitchellh/iochan	1.0.0
github.com/mitchellh/mapstructure	1.4.1
github.com/modern-go/concurrent	0.0.0-20180306012644-bacd9c7ef1dd
github.com/modern-go/reflect2	1.0.1
github.com/modern-go/reflect2	1.0.2
github.com/mtibben/percent	0.2.1
github.com/mwitkow/go-conntrack	0.0.0-20190716064945-2f068394615f
github.com/nxadm/tail	1.4.4
github.com/onsi/ginkgo	1.14.0
github.com/onsi/gomega	1.10.1
github.com/opentracing/opentracing-go	1.2.0
github.com/pascaldekloe/goe	0.0.0-20180627143212-57f6aae5913c
github.com/pelletier/go-toml	1.9.3
github.com/pierrec/lz4	2.0.5+incompatible
github.com/pkg/errors	0.9.1
github.com/pkg/sftp	1.10.1
github.com/pmezard/go-difflib	1.0.0
github.com/posener/complete	1.1.1
github.com/prometheus/client_golang	1.12.2
github.com/prometheus/client_model	0.2.0
github.com/prometheus/common	0.32.1
github.com/prometheus/procfs	0.7.3
github.com/rogpeppe/fastuuid	1.2.0
github.com/rogpeppe/go-internal	1.3.0
github.com/russross/blackfriday/v2	2.0.1
github.com/ryanuber/columnize	0.0.0-20160712163229-9b3edd62028f
github.com/sean-/seed	0.0.0-20170313163322-e2103e2c3529
github.com/shurcooL/sanitized_anchor_name	1.0.0

github.com/sirupsen/logrus	1.6.0
github.com/smartystreets/assertions	0.0.0-20180927180507-b2de0cb4f26d
github.com/smartystreets/goconvey	1.6.4
github.com/spaolacci/murmur3	1.1.0
github.com/spf13/afero	1.6.0
github.com/spf13/cast	1.3.1
github.com/spf13/cobra	1.2.1
github.com/spf13/jwalterweatherman	1.1.0
github.com/spf13/pflag	1.0.5
github.com/spf13/viper	1.8.1
github.com/stretchr/objx	0.2.0
github.com/stretchr/testify	1.7.0
github.com/subosito/gotenv	1.2.0
github.com/yuin/goldmark	1.3.5
go.etcd.io/etcd/api/v3	3.5.0
go.etcd.io/etcd/client/pkg/v3	3.5.0
go.etcd.io/etcd/client/v2	2.305.0
go.opencensus.io	0.23.0
go.uber.org/atomic	1.7.0
go.uber.org/multierr	1.6.0
go.uber.org/zap	1.17.0
golang.org/x/crypto	0.0.0-20200622213623-75b288015ac9
golang.org/x/exp	0.0.0-20200224162631-6cc2880d07d6
golang.org/x/image	0.0.0-20190802002840-cff245a6509b
golang.org/x/lint	0.0.0-20210508222113-6edffad5e616
golang.org/x/mobile	0.0.0-20190719004257-d2bd2a29d028
golang.org/x/mod	0.4.2
golang.org/x/net	0.0.0-20210726213435-c6fcb2dbf985
golang.org/x/oauth2	0.0.0-20210402161424-2e8d93401602
golang.org/x/oauth2	0.0.0-20210514164344-f6687ab2804c
golang.org/x/sync	0.0.0-20210220032951-036812b2e83c
golang.org/x/sys	0.0.0-20210603081109-ebe580a85c40
golang.org/x/sys	0.0.0-20220114195835-da31bd327af9

golang.org/x/term	0.0.0-20201126162022-7de9c90e9dd1
golang.org/x/text	0.3.6
golang.org/x/time	0.0.0-20191024005414-555d28b269f0
golang.org/x/tools	0.1.2
golang.org/x/xerrors	0.0.0-20200804184101-5ec99f83aff1
google.golang.org/api	0.44.0
google.golang.org/appengine	1.6.7
google.golang.org/genproto	0.0.0-20210602131652-f16073e35f0c
google.golang.org/grpc	1.38.0
google.golang.org/protobuf	1.26.0
gopkg.in/alecthomas/kingpin.v2	2.2.6
gopkg.in/check.v1	1.0.0-20190902080502-41f04d3bba15
gopkg.in/errgo.v2	2.1.0
gopkg.in/fsnotify.v1	1.4.7
gopkg.in/ini.v1	1.62.0
gopkg.in/natefinch/lumberjack.v2	2.0.0
gopkg.in/square/go-jose.v2	2.4.1
gopkg.in/tomb.v1	1.0.0-20141024135613-dd632973f1e7
gopkg.in/yaml.v2	2.4.0
gopkg.in/yaml.v3	3.0.0-20210107192922-496545a6307b
honnef.co/go/tools	0.0.1-2020.1.4
rsc.io/binaryregexp	0.2.0
rsc.io/quote/v3	3.1.0
rsc.io/sampler	1.3.0
aopalliance:aopalliance	1.0
ch.qos.logback:logback-core	1.2.3
ch.qos.reload4j:reload4j	1.2.18.3
ch.qos.reload4j:reload4j	1.2.22
co.elastic.clients:elasticsearch-java	8.5.2
com.101tec:zkclient	0.10
com.aerospike:aerospike-client-bc	4.4.20
com.alibaba.otter:canal.client	1.1.5
com.alibaba.otter:canal.common	1.1.5

com.alibaba.otter:canal.protocol	1.1.5
com.alibaba:fastjson	1.2.83
com.amazonaws:amazon-kinesis-client	1.13.3
com.amazonaws:amazon-kinesis-producer	0.14.0
com.amazonaws:aws-java-sdk-cloudwatch	1.12.262
com.amazonaws:aws-java-sdk-core	1.12.262
com.amazonaws:aws-java-sdk-dynamodb	1.12.262
com.amazonaws:aws-java-sdk-kinesis	1.12.262
com.amazonaws:aws-java-sdk-kms	1.12.262
com.amazonaws:aws-java-sdk-s3	1.12.262
com.amazonaws:aws-java-sdk-sts	1.12.262
com.amazonaws:dynamodb-streams-kinesis-adapter	1.5.1
com.amazonaws:jmespath-java	1.12.262
com.auth0:java-jwt	4.3.0
com.auth0:jwks-rsa	0.22.0
com.beust:jcommander	1.82
com.carrotsearch:hppc	0.9.1
com.clearspring.analytics:stream	2.9.5
com.cronutils:cron-utils	9.1.6
com.datastax.cassandra:cassandra-driver-core	3.11.2
com.dslplatform:dsl-json	1.8.4
com.esri.geometry:esri-geometry-api	2.2.4
com.fasterxml.jackson.core:jackson-annotations	2.14.2
com.fasterxml.jackson.core:jackson-core	2.14.2
com.fasterxml.jackson.core:jackson-databind	2.14.2
com.fasterxml.jackson.dataformat:jackson-dataformat-cbor	2.14.2
com.fasterxml.jackson.dataformat:jackson-dataformat-smile	2.14.2
com.fasterxml.jackson.dataformat:jackson-dataformat-yaml	2.14.2
com.fasterxml.jackson.datatype:jackson-datatype-guava	2.14.2
com.fasterxml.jackson.datatype:jackson-datatype-jdk8	2.14.2
com.fasterxml.jackson.datatype:jackson-datatype-joda	2.14.2
com.fasterxml.jackson.datatype:jackson-datatype-jsr310	2.14.2
com.fasterxml.jackson.jaxrs:jackson-jaxrs-base	2.14.2

com.fasterxml.jackson.jaxrs:jackson-jaxrs-json-provider	2.14.2
com.fasterxml.jackson.module:jackson-module-jaxb-annotations	2.14.2
com.fasterxml.jackson.module:jackson-module-jsonSchema	2.14.2
com.fasterxml.jackson.module:jackson-module-parameter-names	2.14.2
com.fasterxml.woodstox:woodstox-core	5.4.0
com.github.ben-manes.caffeine:caffeine	2.9.1
com.github.jnr:jffi	1.2.16
com.github.jnr:jnr-constants	0.9.9
com.github.jnr:jnr-ffi	2.1.7
com.github.jnr:jnr-posix	3.0.44
com.github.jnr:jnr-x86asm	1.0.2
com.github.luben:zstd-jni	1.5.2-3
com.github.oshi:oshi-core-java11	6.4.0
com.github.oshi:oshi-core	5.8.5
com.github.pjfanning:jersey-json	1.20
com.github.scribejava:scribejava-apis	6.9.0
com.github.scribejava:scribejava-core	6.9.0
com.github.seancfoley:ipaddress	5.3.3
com.github.stephenc.jcip:jcip-annotations	1.0-1
com.github.wnameless.json:json-base	2.0.0
com.github.wnameless.json:json-flattener	0.13.0
com.github.zafarkhaja:java-semver	0.9.0
com.google.api.grpc:proto-google-common-protos	2.0.1
com.google.api.grpc:proto-google-common-protos	2.9.0
com.google.auth:google-auth-library-credentials	1.4.0
com.google.auth:google-auth-library-oauth2-http	1.4.0
com.google.auto.value:auto-value-annotations	1.9
com.google.code.findbugs:jsr305	1.3.9
com.google.code.findbugs:jsr305	3.0.2
com.google.code.gson:gson	2.8.9
com.google.errorprone:error_prone_annotations	2.5.1
com.google.flatbuffers:flatbuffers-java	1.9.0
com.google.guava:failureaccess	1.0.1

com.google.guava:guava	32.1.2-jre
com.google.guava:listenablefuture	9999.0-empty-to-avoid-conflict-with-guava
com.google.http-client:google-http-client-gson	1.41.0
com.google.http-client:google-http-client	1.41.0
com.google.inject.extensions:guice-assistedinject	5.1.0
com.google.inject:guice	4.2.3
com.google.inject:guice	5.1.0
com.google.j2objc:j2objc-annotations	1.3
com.google.protobuf:protobuf-java-util	3.19.6
com.google.protobuf:protobuf-java	3.19.6
com.google.re2j:re2j	1.1
com.google.re2j:re2j	1.6
com.googlecode.json-simple:json-simple	1.1.1
com.influxdb:influxdb-client-core	4.0.0
com.influxdb:influxdb-client-java	4.0.0
com.influxdb:influxdb-client-utils	4.0.0
com.jcraft:jsch	0.1.55
com.microsoft.sqlserver:mssql-jdbc	9.4.1.jre8
com.nimbusds:nimbus-jose-jwt	7.9
com.nimbusds:nimbus-jose-jwt	9.8.1
com.rabbitmq:amqp-client	5.5.3
com.sproutsocial:nsq-j	1.0
com.squareup.moshi:moshi	1.8.0
com.squareup.okhttp:okhttp	2.7.5
com.squareup.okhttp3:logging-interceptor	3.14.9
com.squareup.okhttp3:logging-interceptor	4.9.3
com.squareup.okhttp3:okhttp-urlconnection	3.14.9
com.squareup.okhttp3:okhttp	3.14.9
com.squareup.okhttp3:okhttp	4.9.3
com.squareup.okio:okio-jvm	3.4.0
com.squareup.okio:okio	1.17.2
com.squareup.okio:okio	3.4.0
com.squareup.retrofit2:converter-gson	2.9.0

com.squareup.retrofit2:converter-moshi	2.9.0
com.squareup.retrofit2:converter-scalars	2.9.0
com.squareup.retrofit2:retrofit	2.9.0
com.sun.activation:javax.activation	1.2.0
com.sun.jersey:jersey-client	1.9
com.sun.jersey:jersey-core	1.19.4
com.sun.jersey:jersey-server	1.19.4
com.sun.jersey:jersey-servlet	1.19.4
com.sun.xml.bind:jaxb-impl	2.2.3-1
com.sun.xml.bind:jaxb-impl	2.3.3
com.teradata:re2j-td	1.4
com.thoughtworks.paranamer:paranamer	2.7
com.twitter.common:objectsize	0.0.12
com.twitter:hbc-core	2.2.0
com.twitter:joauth	6.0.2
com.typesafe.netty:netty-reactive-streams-http	2.0.4
com.typesafe.netty:netty-reactive-streams	2.0.4
com.typesafe.netty:netty-reactive-streams	2.0.6
com.yahoo.athenz:athenz-cert-refresher	1.10.50
com.yahoo.athenz:athenz-zpe-java-client	1.10.50
com.yahoo.athenz:athenz-zts-java-client-core	1.10.50
com.yahoo.datasketches:sketches-core	0.8.3
com.yahoo.rdl:rdl-java	1.5.4
com.zaxxer:HikariCP-java7	2.4.12
com.zendesk:mysql-binlog-connector-java	0.27.2
commons-beanutils:commons-beanutils	1.9.4
commons-cli:commons-cli	1.5.0
commons-codec:commons-codec	1.15
commons-collections:commons-collections	3.2.2
commons-configuration:commons-configuration	1.10
commons-dbcp:commons-dbcp	1.4
commons-io:commons-io	2.8.0
commons-lang:commons-lang	2.6

commons-logging:commons-logging	1.1.1
commons-logging:commons-logging	1.1.3
commons-net:commons-net	3.1
commons-net:commons-net	3.9.0
commons-pool:commons-pool	1.5.4
dnsjava:dnsjava	2.1.7
info.picocli:picocli	4.6.1
io.airlift.discovery:discovery-server	1.30
io.airlift:aircompressor	0.20
io.airlift:bootstrap	213
io.airlift:bytecode	1.2
io.airlift:concurrent	213
io.airlift:configuration	213
io.airlift:discovery	213
io.airlift:event-http	213
io.airlift:event	213
io.airlift:http-client	213
io.airlift:http-server	213
io.airlift:jaxrs	213
io.airlift:jmx-http-rpc	213
io.airlift:jmx-http	213
io.airlift:jmx	213
io.airlift:joni	2.1.5.3
io.airlift:json	213
io.airlift:launcher	213
io.airlift:log-manager	213
io.airlift:log	213
io.airlift:node	213
io.airlift:parameternames	1.4
io.airlift:security	213
io.airlift:slice	0.41
io.airlift:stats	213
io.airlift:trace-token	213

io.airlift:units	1.6
io.codearte.jfairy:jfairy	0.5.9
io.confluent:kafka-avro-serializer	6.2.8
io.confluent:kafka-connect-avro-converter	6.2.8
io.confluent:kafka-schema-registry-client	6.2.8
io.debezium:debezium-api	1.9.7.Final
io.debezium:debezium-connector-mongodb	1.9.7.Final
io.debezium:debezium-connector-mysql	1.9.7.Final
io.debezium:debezium-connector-oracle	1.9.7.Final
io.debezium:debezium-connector-postgres	1.9.7.Final
io.debezium:debezium-connector-sqlserver	1.9.7.Final
io.debezium:debezium-core	1.9.7.Final
io.debezium:debezium-ddl-parser	1.9.7.Final
io.dropwizard.metrics:metrics-core	4.1.12.1
io.dropwizard.metrics:metrics-graphite	4.1.12.1
io.dropwizard.metrics:metrics-jmx	4.1.11
io.dropwizard.metrics:metrics-jmx	4.1.12.1
io.dropwizard.metrics:metrics-jvm	4.1.11
io.dropwizard.metrics:metrics-jvm	4.1.12.1
io.etcd:jetcd-api	0.7.5
io.etcd:jetcd-common	0.7.5
io.etcd:jetcd-core	0.7.5
io.etcd:jetcd-grpc	0.7.5
io.grpc:grpc-all	1.55.3
io.grpc:grpc-alts	1.55.3
io.grpc:grpc-api	1.37.0
io.grpc:grpc-api	1.55.3
io.grpc:grpc-auth	1.55.3
io.grpc:grpc-context	1.37.0
io.grpc:grpc-context	1.55.3
io.grpc:grpc-core	1.37.0
io.grpc:grpc-core	1.55.3
io.grpc:grpc-grpclb	1.55.3

io.grpc:grpc-netty-shaded	1.55.3
io.grpc:grpc-netty	1.37.0
io.grpc:grpc-netty	1.55.3
io.grpc:grpc-protobuf-lite	1.37.0
io.grpc:grpc-protobuf-lite	1.55.3
io.grpc:grpc-protobuf	1.37.0
io.grpc:grpc-protobuf	1.55.3
io.grpc:grpc-rls	1.55.3
io.grpc:grpc-services	1.55.3
io.grpc:grpc-servlet-jakarta	1.55.3
io.grpc:grpc-servlet	1.55.3
io.grpc:grpc-stub	1.37.0
io.grpc:grpc-stub	1.55.3
io.grpc:grpc-xds	1.55.3
io.gsonfire:gson-fire	1.8.4
io.gsonfire:gson-fire	1.8.5
io.jsonwebtoken:jjwt-api	0.11.1
io.jsonwebtoken:jjwt-impl	0.11.1
io.jsonwebtoken:jjwt-jackson	0.11.1
io.kubernetes:client-java-api	18.0.0
io.kubernetes:client-java-proto	18.0.0
io.kubernetes:client-java	18.0.0
io.lettuce:lettuce-core	5.0.2.RELEASE
io.netty.incubator:netty-incubator-transport-classes-io_uring	0.0.21.Final
io.netty.incubator:netty-incubator-transport-native-io_uring	0.0.21.Final
io.netty:netty-all	4.1.94.Final
io.netty:netty-buffer	4.1.94.Final
io.netty:netty-codec-dns	4.1.94.Final
io.netty:netty-codec-haproxy	4.1.94.Final
io.netty:netty-codec-http2	4.1.94.Final
io.netty:netty-codec-http	4.1.94.Final
io.netty:netty-codec-memcache	4.1.94.Final
io.netty:netty-codec-mqtt	4.1.94.Final

io.netty:netty-codec-redis	4.1.94.Final
io.netty:netty-codec-smtp	4.1.94.Final
io.netty:netty-codec-socks	4.1.94.Final
io.netty:netty-codec-stomp	4.1.94.Final
io.netty:netty-codec-xml	4.1.94.Final
io.netty:netty-codec	4.1.94.Final
io.netty:netty-common	4.1.94.Final
io.netty:netty-handler-proxy	4.1.94.Final
io.netty:netty-handler-ssl-ocsp	4.1.94.Final
io.netty:netty-handler	4.1.94.Final
io.netty:netty-resolver-dns-classes-macos	4.1.94.Final
io.netty:netty-resolver-dns-native-macos	4.1.94.Final
io.netty:netty-resolver-dns	4.1.94.Final
io.netty:netty-resolver	4.1.94.Final
io.netty:netty-tcnative-boringssl-static	2.0.61.Final
io.netty:netty-tcnative-classes	2.0.61.Final
io.netty:netty-transport-classes-epoll	4.1.94.Final
io.netty:netty-transport-classes-kqueue	4.1.94.Final
io.netty:netty-transport-native-epoll	4.1.94.Final
io.netty:netty-transport-native-unix-common	4.1.94.Final
io.netty:netty-transport-rxtx	4.1.94.Final
io.netty:netty-transport-sctp	4.1.94.Final
io.netty:netty-transport-udt	4.1.94.Final
io.netty:netty-transport	4.1.94.Final
io.opencensus:opencensus-api	0.28.0
io.opencensus:opencensus-contrib-http-util	0.28.0
io.opencensus:opencensus-proto	0.2.0
io.perfmark:perfmark-api	0.26.0
io.projectreactor:reactor-core	3.1.4.RELEASE
io.prometheus.jmx:collector	0.16.1
io.prometheus:simpleclient	0.16.0
io.prometheus:simpleclient_caffeine	0.16.0
io.prometheus:simpleclient_common	0.16.0

io.prometheus:simpleclient_hotspot	0.16.0
io.prometheus:simpleclient_httpserver	0.16.0
io.prometheus:simpleclient_jetty	0.16.0
io.prometheus:simpleclient_log4j2	0.16.0
io.prometheus:simpleclient_servlet	0.16.0
io.prometheus:simpleclient_servlet_common	0.16.0
io.prometheus:simpleclient_tracer_common	0.16.0
io.prometheus:simpleclient_tracer_otel	0.16.0
io.prometheus:simpleclient_tracer_otel_agent	0.16.0
io.reactivex.rxjava2:rxjava	2.1.14
io.reactivex.rxjava2:rxjava	2.2.19
io.reactivex.rxjava3:rxjava	3.0.1
io.reactivex.rxjava3:rxjava	3.0.4
io.swagger:swagger-annotations	1.6.2
io.swagger:swagger-core	1.6.2
io.trino:trino-array	368
io.trino:trino-cli	368
io.trino:trino-client	368
io.trino:trino-geospatial-toolkit	368
io.trino:trino-main	368
io.trino:trino-matching	368
io.trino:trino-memory-context	368
io.trino:trino-parser	368
io.trino:trino-plugin-toolkit	368
io.trino:trino-record-decoder	368
io.trino:trino-server-main	368
io.trino:trino-spi	368
io.vertx:vertx-auth-common	4.3.8
io.vertx:vertx-bridge-common	4.3.8
io.vertx:vertx-core	4.3.8
io.vertx:vertx-grpc	4.3.5
io.vertx:vertx-web-common	4.3.8
io.vertx:vertx-web	4.3.8

it.unimi.dsi:fastutil	8.3.0
jakarta.activation:jakarta.activation-api	1.2.2
jakarta.annotation:jakarta.annotation-api	1.3.5
jakarta.json:jakarta.json-api	2.0.1
jakarta.validation:jakarta.validation-api	2.0.2
jakarta.ws.rs:jakarta.ws.rs-api	2.1.6
jakarta.xml.bind:jakarta.xml.bind-api	2.3.3
javax.activation:javax.activation-api	1.2.0
javax.annotation:javax.annotation-api	1.3.2
javax.inject:javax.inject	1
javax.servlet:javax.servlet-api	3.1.0
javax.servlet:javax.servlet-api	4.0.1
javax.validation:validation-api	1.1.0.Final
javax.validation:validation-api	2.0.1.Final
javax.websocket:javax.websocket-client-api	1.0
javax.ws.rs:javax.ws.rs-api	2.1
javax.ws.rs:jsr311-api	1.1.1
javax.xml.bind:jaxb-api	2.3.0
javax.xml.bind:jaxb-api	2.3.1
jline:jline	2.14.6
joda-time:joda-time	2.10.10
mysql:mysql-connector-java	8.0.30
net.bytebuddy:byte-buddy-agent	1.11.13
net.bytebuddy:byte-buddy	1.10.22
net.bytebuddy:byte-buddy	1.11.13
net.java.dev.jna:jna-jpms	5.12.1
net.java.dev.jna:jna-platform-jpms	5.12.1
net.java.dev.jna:jna-platform	5.10.0
net.java.dev.jna:jna	5.12.1
net.jcip:jcip-annotations	1.0
net.jodah:failsafe	2.4.0
net.jodah:failsafe	2.4.4
net.jodah:typetools	0.5.0

net.minidev:accessors-smart	2.4.9
net.minidev:json-smart	2.4.10
net.sf.opencsv:opencsv	2.3
org.alluxio:alluxio-core-client-fs	2.7.3
org.alluxio:alluxio-core-common	2.7.3
org.alluxio:alluxio-core-transport	2.7.3
org.antlr:antlr4-runtime	4.8
org.antlr:antlr4-runtime	4.9.2
org.apache.ant:ant-launcher	1.10.12
org.apache.ant:ant	1.10.12
org.apache.avro:avro-ipc	1.8.2
org.apache.avro:avro-protobuf	1.10.2
org.apache.avro:avro	1.10.2
org.apache.avro:avro	1.8.2
org.apache.bookkeeper.http:http-server	4.16.2
org.apache.bookkeeper.http:vertx-http-server	4.16.2
org.apache.bookkeeper.stats:bookkeeper-stats-api	4.16.2
org.apache.bookkeeper.stats:codahale-metrics-provider	4.16.2
org.apache.bookkeeper.stats:prometheus-metrics-provider	4.16.2
org.apache.bookkeeper:bookkeeper-common-allocator	4.16.2
org.apache.bookkeeper:bookkeeper-common	4.16.2
org.apache.bookkeeper:bookkeeper-server	4.16.2
org.apache.bookkeeper:bookkeeper-tools-framework	4.16.2
org.apache.bookkeeper:circe-checksum	4.16.2
org.apache.bookkeeper:cpu-affinity	4.16.2
org.apache.bookkeeper:stream-storage-java-client	4.16.2
org.apache.bookkeeper:stream-storage-server	4.16.2
org.apache.bval:bval-jsr	2.0.5
org.apache.commons:commons-collections4	4.4
org.apache.commons:commons-compress	1.21
org.apache.commons:commons-configuration2	2.8.0
org.apache.commons:commons-crypto	1.0.0
org.apache.commons:commons-csv	1.8

org.apache.commons:commons-lang3	3.11
org.apache.commons:commons-math3	3.1.1
org.apache.commons:commons-math3	3.6.1
org.apache.commons:commons-text	1.10.0
org.apache.curator:curator-client	2.13.0
org.apache.curator:curator-client	4.2.0
org.apache.curator:curator-client	5.1.0
org.apache.curator:curator-framework	2.13.0
org.apache.curator:curator-framework	4.2.0
org.apache.curator:curator-framework	5.1.0
org.apache.curator:curator-recipes	5.1.0
org.apache.derby:derby	10.14.1.0
org.apache.directory.api:api-asn1-api	1.0.0-M20
org.apache.directory.api:api-util	1.0.0-M20
org.apache.directory.server:apacheds-kerberos-codec	2.0.0-M15
org.apache.distributedlog:distributedlog-core	4.16.2
org.apache.flume.flume-ng-channels:flume-file-channel	1.9.0
org.apache.flume.flume-ng-channels:flume-jdbc-channel	1.9.0
org.apache.flume.flume-ng-channels:flume-spillable-memory-channel	1.9.0
org.apache.flume.flume-ng-configfilters:flume-ng-config-filter-api	1.9.0
org.apache.flume.flume-ng-sinks:flume-hdfs-sink	1.9.0
org.apache.flume.flume-ng-sinks:flume-irc-sink	1.9.0
org.apache.flume:flume-ng-auth	1.9.0
org.apache.flume:flume-ng-configuration	1.9.0
org.apache.flume:flume-ng-core	1.9.0
org.apache.flume:flume-ng-node	1.9.0
org.apache.flume:flume-ng-sdk	1.9.0
org.apache.geronimo.specs:geronimo-jcache_1.0_spec	1.0-alpha-1
org.apache.hadoop.thirdparty:hadoop-shaded-guava	1.1.1
org.apache.hadoop.thirdparty:hadoop-shaded-protobuf_3_7	1.1.1
org.apache.hadoop:hadoop-annotations	3.3.5
org.apache.hadoop:hadoop-auth	2.10.2
org.apache.hadoop:hadoop-auth	3.3.5

org.apache.hadoop:hadoop-client	2.10.2
org.apache.hadoop:hadoop-client	3.3.5
org.apache.hadoop:hadoop-common	2.10.2
org.apache.hadoop:hadoop-common	3.3.5
org.apache.hadoop:hadoop-hdfs-client	2.10.2
org.apache.hadoop:hadoop-hdfs-client	3.3.5
org.apache.hadoop:hadoop-mapreduce-client-app	2.10.2
org.apache.hadoop:hadoop-mapreduce-client-common	2.10.2
org.apache.hadoop:hadoop-mapreduce-client-common	3.3.5
org.apache.hadoop:hadoop-mapreduce-client-core	2.10.2
org.apache.hadoop:hadoop-mapreduce-client-core	3.3.5
org.apache.hadoop:hadoop-mapreduce-client-jobclient	2.10.2
org.apache.hadoop:hadoop-mapreduce-client-jobclient	3.3.5
org.apache.hadoop:hadoop-mapreduce-client-shuffle	2.10.2
org.apache.hadoop:hadoop-yarn-api	2.10.2
org.apache.hadoop:hadoop-yarn-client	2.10.2
org.apache.hadoop:hadoop-yarn-client	3.3.5
org.apache.hadoop:hadoop-yarn-common	2.10.2
org.apache.hadoop:hadoop-yarn-registry	2.10.2
org.apache.hadoop:hadoop-yarn-server-common	2.10.2
org.apache.hbase.thirdparty:hbase-shaded-gson	4.1.4
org.apache.hbase.thirdparty:hbase-shaded-miscellaneous	4.1.4
org.apache.hbase.thirdparty:hbase-shaded-netty	4.1.4
org.apache.hbase.thirdparty:hbase-shaded-protobuf	4.1.4
org.apache.hbase.thirdparty:hbase-unsafe	4.1.4
org.apache.hbase:hbase-client	2.4.16
org.apache.hbase:hbase-common	2.4.16
org.apache.hbase:hbase-hadoop-compat	2.4.16
org.apache.hbase:hbase-hadoop2-compat	2.4.16
org.apache.hbase:hbase-logging	2.4.16
org.apache.hbase:hbase-metrics-api	2.4.16
org.apache.hbase:hbase-metrics	2.4.16
org.apache.hbase:hbase-protocol-shaded	2.4.16

org.apache.hbase:hbase-protocol	2.4.16
org.apache.htrace:htrace-core4	4.1.0-incubating
org.apache.htrace:htrace-core4	4.2.0-incubating
org.apache.httpcomponents:httpclient	4.5.13
org.apache.httpcomponents:httpcore	4.4.15
org.apache.httpcomponents:httpmime	4.5.13
org.apache.jclouds.api:atmos	2.5.0
org.apache.jclouds.api:glacier	2.5.0
org.apache.jclouds.api:oauth	2.5.0
org.apache.jclouds.api:openstack-keystone	2.5.0
org.apache.jclouds.api:openstack-swift	2.5.0
org.apache.jclouds.api:s3	2.5.0
org.apache.jclouds.api:sts	2.5.0
org.apache.jclouds.common:googlecloud	2.5.0
org.apache.jclouds.driver:jclouds-apachehc	2.5.0
org.apache.jclouds.driver:jclouds-okhttp	2.5.0
org.apache.jclouds.driver:jclouds-slf4j	2.5.0
org.apache.jclouds.provider:aws-s3	2.5.0
org.apache.jclouds.provider:azureblob	2.5.0
org.apache.jclouds.provider:b2	2.5.0
org.apache.jclouds.provider:google-cloud-storage	2.5.0
org.apache.jclouds.provider:rackspace-cloudfiles-uk	2.5.0
org.apache.jclouds.provider:rackspace-cloudfiles-us	2.5.0
org.apache.jclouds:jclouds-allblobstore	2.5.0
org.apache.jclouds:jclouds-blobstore	2.5.0
org.apache.jclouds:jclouds-core	2.5.0
org.apache.kafka:connect-api	3.4.0
org.apache.kafka:connect-json	3.4.0
org.apache.kafka:connect-runtime	3.4.0
org.apache.kafka:connect-transforms	3.4.0
org.apache.kafka:kafka-clients	3.4.0
org.apache.kerby:kerb-admin	1.0.1
org.apache.kerby:kerb-client	1.0.1

org.apache.kerby:kerb-common	1.0.1
org.apache.kerby:kerb-core	1.0.1
org.apache.kerby:kerb-crypto	1.0.1
org.apache.kerby:kerb-identity	1.0.1
org.apache.kerby:kerb-server	1.0.1
org.apache.kerby:kerb-simplekdc	1.0.1
org.apache.kerby:kerb-util	1.0.1
org.apache.kerby:kerby-asn1	1.0.1
org.apache.kerby:kerby-config	1.0.1
org.apache.kerby:kerby-pkix	1.0.1
org.apache.kerby:kerby-util	1.0.1
org.apache.kerby:kerby-xdr	1.0.1
org.apache.kerby:token-provider	1.0.1
org.apache.logging.log4j:log4j-api	2.17.1
org.apache.logging.log4j:log4j-api	2.18.0
org.apache.logging.log4j:log4j-core	2.17.1
org.apache.logging.log4j:log4j-core	2.18.0
org.apache.logging.log4j:log4j-slf4j-impl	2.17.1
org.apache.logging.log4j:log4j-slf4j-impl	2.18.0
org.apache.logging.log4j:log4j-web	2.18.0
org.apache.lucene:lucene-analyzers-common	8.4.1
org.apache.lucene:lucene-core	8.4.1
org.apache.mina:mina-core	2.0.4
org.apache.pulsar.tests:bc_2_0_0	3.1.0-SNAPSHOT
org.apache.pulsar.tests:bc_2_0_1	3.1.0-SNAPSHOT
org.apache.pulsar.tests:bc_2_6_0	3.1.0-SNAPSHOT
org.apache.pulsar.tests:docker-images	3.1.0-SNAPSHOT
org.apache.pulsar.tests:integration	3.1.0-SNAPSHOT
org.apache.pulsar.tests:java-test-functions	3.1.0-SNAPSHOT
org.apache.pulsar.tests:java-test-image	3.1.0-SNAPSHOT
org.apache.pulsar.tests:java-test-plugins	3.1.0-SNAPSHOT
org.apache.pulsar.tests:latest-version-image	3.1.0-SNAPSHOT
org.apache.pulsar.tests:pulsar-client-admin-shade-test	3.1.0-SNAPSHOT

org.apache.pulsar.tests:pulsar-client-all-shade-test	3.1.0-SNAPSHOT
org.apache.pulsar.tests:pulsar-client-shade-test	3.1.0-SNAPSHOT
org.apache.pulsar.tests:tests-parent	3.1.0-SNAPSHOT
org.apache.pulsar:bcfips-include-test	3.1.0-SNAPSHOT
org.apache.pulsar:bouncy-castle-bc	3.1.0-SNAPSHOT
org.apache.pulsar:bouncy-castle-bcfips	3.1.0-SNAPSHOT
org.apache.pulsar:bouncy-castle-parent	3.1.0-SNAPSHOT
org.apache.pulsar:buildtools	3.1.0-SNAPSHOT
org.apache.pulsar:distribution	3.1.0-SNAPSHOT
org.apache.pulsar:docker-images	3.1.0-SNAPSHOT
org.apache.pulsar:jclouds-shaded	3.1.0-SNAPSHOT
org.apache.pulsar:managed-ledger	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-all-docker-image	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-broker-auth-athenz	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-broker-auth-oidc	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-broker-auth-sasl	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-broker-common	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-broker	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-cli-utils	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-1x-base	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-1x	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-2x-shaded	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-admin-api	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-admin-original	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-admin	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-all	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-api	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-auth-athenz	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-auth-sasl	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-messagecrypto-bc	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-original	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-tools-api	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-tools-customcommand-example	3.1.0-SNAPSHOT

org.apache.pulsar:pulsar-client-tools-test	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client-tools	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-client	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-common	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-config-validation	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-docker-image	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-docs-tools	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-api-examples-builtin	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-api-examples	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-api	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-instance	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-local-runner-original	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-local-runner	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-proto	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-runtime-all	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-runtime	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-secrets	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-utils	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions-worker	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-functions	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-aerospike	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-alluxio	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-aws	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-batch-data-generator	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-batch-discovery-triggerers	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-canal	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-cassandra	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-common	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-core	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-data-generator	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium-core	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium-mongodb	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium-mssql	3.1.0-SNAPSHOT

org.apache.pulsar:pulsar-io-debezium-mysql	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium-oracle	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium-postgres	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-debezium	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-distribution	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-docs	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-dynamodb	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-elastic-search	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-file	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-flume	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-hbase	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-hdfs2	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-hdfs3	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-http	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-influxdb	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-clickhouse	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-core	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-mariadb	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-openmldb	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-postgres	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc-sqlite	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-jdbc	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-kafka-connect-adaptor-nar	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-kafka-connect-adaptor	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-kafka	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-kinesis	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-mongo	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-netty	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-nsq	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-rabbitmq	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-redis	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-solr	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-io-twitter	3.1.0-SNAPSHOT

org.apache.pulsar:pulsar-io	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-metadata	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-offloader-distribution	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-package-bookkeeper-storage	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-package-core	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-package-filesystem-storage	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-package-management	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-presto-connector-original	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-presto-connector	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-presto-distribution	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-proxy	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-server-distribution	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-shell-distribution	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-sql	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-testclient	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-transaction-common	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-transaction-coordinator	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-transaction-parent	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar-websocket	3.1.0-SNAPSHOT
org.apache.pulsar:pulsar	3.1.0-SNAPSHOT
org.apache.pulsar:structured-event-log	3.1.0-SNAPSHOT
org.apache.pulsar:testmocks	3.1.0-SNAPSHOT
org.apache.pulsar:tiered-storage-file-system	3.1.0-SNAPSHOT
org.apache.pulsar:tiered-storage-jcloud	3.1.0-SNAPSHOT
org.apache.pulsar:tiered-storage-parent	3.1.0-SNAPSHOT
org.apache.solr:solr-solrj	8.11.1
org.apache.thrift:libthrift	0.14.2
org.apache.thrift:libthrift	0.9.3
org.apache.velocity:velocity	1.7
org.apache.yetus:audience-annotations	0.12.0
org.apache.yetus:audience-annotations	0.13.0
org.apache.zookeeper:zookeeper-jute	3.8.1
org.apache.zookeeper:zookeeper-prometheus-metrics	3.8.1

org.apache.zookeeper:zookeeper	3.8.1
org.assertj:assertj-core	3.24.2
org.asynchttpclient:async-http-client-netty-utils	2.12.1
org.asynchttpclient:async-http-client	2.12.1
org.bitbucket.b_c:jose4j	0.9.3
org.bouncycastle:bc-fips	1.0.2.3
org.bouncycastle:bcpkix-fips	1.0.6
org.bouncycastle:bcpkix-jdk18on	1.75
org.bouncycastle:bcprov-ext-jdk18on	1.75
org.bouncycastle:bcprov-jdk18on	1.75
org.bouncycastle:bcutil-jdk18on	1.75
org.checkerframework:checker-qual	3.10.0
org.checkerframework:checker-qual	3.33.0
org.codehaus.jackson:jackson-core-asl	1.9.13
org.codehaus.jackson:jackson-jaxrs	1.9.13
org.codehaus.jackson:jackson-mapper-asl	1.9.13
org.codehaus.jackson:jackson-xc	1.9.13
org.codehaus.jettison:jettison	1.5.4
org.codehaus.woodstox:stax2-api	4.2.1
org.conscrypt:conscrypt-openjdk-uber	2.5.2
org.eclipse.jetty.http2:http2-client	9.4.51.v20230217
org.eclipse.jetty.http2:http2-common	9.4.51.v20230217
org.eclipse.jetty.http2:http2-hpack	9.4.51.v20230217
org.eclipse.jetty.http2:http2-http-client-transport	9.4.51.v20230217
org.eclipse.jetty.http2:http2-server	9.4.51.v20230217
org.eclipse.jetty.websocket:javax-websocket-client-impl	9.4.51.v20230217
org.eclipse.jetty.websocket:websocket-api	9.4.51.v20230217
org.eclipse.jetty.websocket:websocket-client	9.4.51.v20230217
org.eclipse.jetty.websocket:websocket-common	9.4.51.v20230217
org.eclipse.jetty.websocket:websocket-server	9.4.51.v20230217
org.eclipse.jetty.websocket:websocket-servlet	9.4.51.v20230217
org.eclipse.jetty:jetty-alpn-client	9.4.51.v20230217
org.eclipse.jetty:jetty-alpn-conscrypt-server	9.4.51.v20230217

org.eclipse.jetty:jetty-alpn-java-client	9.4.51.v20230217
org.eclipse.jetty:jetty-alpn-server	9.4.51.v20230217
org.eclipse.jetty:jetty-client	9.4.51.v20230217
org.eclipse.jetty:jetty-continuation	9.4.51.v20230217
org.eclipse.jetty:jetty-http	9.4.51.v20230217
org.eclipse.jetty:jetty-io	9.4.51.v20230217
org.eclipse.jetty:jetty-jmx	9.4.51.v20230217
org.eclipse.jetty:jetty-proxy	9.4.51.v20230217
org.eclipse.jetty:jetty-security	9.4.51.v20230217
org.eclipse.jetty:jetty-server	9.4.51.v20230217
org.eclipse.jetty:jetty-servlet	9.4.51.v20230217
org.eclipse.jetty:jetty-servlets	9.4.51.v20230217
org.eclipse.jetty:jetty-util-ajax	9.4.51.v20230217
org.eclipse.jetty:jetty-util	9.4.51.v20230217
org.eclipse.jetty:jetty-webapp	9.4.51.v20230217
org.eclipse.jetty:jetty-xml	9.4.51.v20230217
org.eclipse.parsson:parsson	1.0.0
org.ehcache:ehcache	3.3.1
org.ehcache:ehcache	3.9.9
org.elasticsearch.client:elasticsearch-rest-client	8.5.2
org.fusesource.leveldbjni:leveldbjni-all	1.8
org.glassfish.hk2.external:aopalliance-repackaged	2.6.1
org.glassfish.hk2.external:jakarta.inject	2.6.1
org.glassfish.hk2:hk2-api	2.6.1
org.glassfish.hk2:hk2-locator	2.6.1
org.glassfish.hk2:hk2-utils	2.6.1
org.glassfish.hk2:osgi-resource-locator	1.0.3
org.glassfish.jersey.connectors:jersey-apache-connector	2.35
org.glassfish.jersey.containers:jersey-container-servlet-core	2.34
org.glassfish.jersey.containers:jersey-container-servlet	2.34
org.glassfish.jersey.core:jersey-client	2.34
org.glassfish.jersey.core:jersey-common	2.34
org.glassfish.jersey.core:jersey-server	2.34

org.glassfish.jersey.ext:jersey-entity-filtering	2.34
org.glassfish.jersey.inject:jersey-hk2	2.34
org.glassfish.jersey.media:jersey-media-json-jackson	2.34
org.glassfish.jersey.media:jersey-media-multipart	2.34
org.hdrhistogram:HdrHistogram	2.1.9
org.iban4j:iban4j	3.2.1
org.infinispan.protostream:protostream-types	4.4.1.Final
org.infinispan.protostream:protostream	4.4.1.Final
org.infinispan:infinispan-client-hotrod	12.1.6.Final
org.infinispan:infinispan-core	12.1.6.Final
org.influxdb:influxdb-java	2.22
org.iq80.leveldb:leveldb-api	0.12
org.iq80.leveldb:leveldb	0.12
org.javassist:javassist	3.25.0-GA
org.jboss.logging:jboss-logging	3.4.1.Final
org.jboss.spec.javax.transaction:jboss-transaction-api_1.2_spec	1.1.1.Final
org.jboss.threads:jboss-threads	2.3.3.Final
org.jctools:jctools-core	2.1.2
org.jetbrains.kotlin:kotlin-stdlib-common	1.8.20
org.jetbrains.kotlin:kotlin-stdlib-jdk7	1.8.20
org.jetbrains.kotlin:kotlin-stdlib-jdk8	1.8.20
org.jetbrains.kotlin:kotlin-stdlib	1.8.20
org.jetbrains:annotations	13.0
org.jgrapht:jgrapht-core	0.9.0
org.jgroups:jgroups	4.2.12.Final
org.jline:jline-reader	3.21.0
org.jline:jline-terminal	3.21.0
org.jline:jline	3.21.0
org.jruby.jcodings:jcodings	1.0.55
org.jruby.joni:joni	2.1.31
org.jvnet.mimepull:mimepull	1.9.13
org.locationtech.jts.io:jts-io-common	1.16.1
org.locationtech.jts:jts-core	1.16.1

org.luaj:luaj-jse	3.0
org.mapdb:mapdb	0.9.9
org.mindrot:jbcrypt	0.4
org.mockito:mockito-core	3.12.4
org.mockito:mockito-inline	3.12.4
org.mongodb:bson	4.1.2
org.mongodb:bson	4.3.3
org.mongodb:mongodb-driver-core	4.1.2
org.mongodb:mongodb-driver-core	4.3.3
org.mongodb:mongodb-driver-reactivestreams	4.1.2
org.mongodb:mongodb-driver-sync	4.3.3
org.mortbay.jetty:jetty-sslengine	6.1.26
org.mortbay.jetty:jetty-util	6.1.26
org.mortbay.jetty:jetty	6.1.26
org.msgpack:msgpack-core	0.9.0
org.objenesis:objenesis	2.6
org.objenesis:objenesis	3.1
org.openjdk.jol:jol-core	0.2
org.opensearch.client:opensearch-rest-client	1.2.4
org.opensearch.client:opensearch-rest-high-level-client	1.2.4
org.opensearch.plugin:aggs-matrix-stats-client	1.2.4
org.opensearch.plugin:lang-mustache-client	1.2.4
org.opensearch.plugin:mapper-extras-client	1.2.4
org.opensearch.plugin:parent-join-client	1.2.4
org.opensearch.plugin:rank-eval-client	1.2.4
org.opensearch:opensearch	1.2.4
org.ow2.asm:asm-analysis	5.0.3
org.ow2.asm:asm-analysis	6.2.1
org.ow2.asm:asm-commons	5.0.3
org.ow2.asm:asm-tree	5.0.3
org.ow2.asm:asm-tree	6.2.1
org.ow2.asm:asm-util	5.0.3
org.ow2.asm:asm-util	6.2.1

org.ow2.asm:asm	5.0.3
org.ow2.asm:asm	9.1
org.ow2.asm:asm	9.3
org.pcollections:pcollections	2.1.2
org.postgresql:postgresql	42.3.5
org.projectlombok:lombok	1.18.28
org.reactivestreams:reactive-streams	1.0.2
org.reactivestreams:reactive-streams	1.0.3
org.reflections:reflections	0.10.2
org.roaringbitmap:RoaringBitmap	0.9.44
org.rocksdb:rocksdbjni	7.9.2
org.schwering:irclib	1.10
org.slf4j:jcl-over-slf4j	1.7.32
org.slf4j:slf4j-api	1.7.30
org.slf4j:slf4j-api	1.7.32
org.slf4j:slf4j-api	1.7.36
org.slf4j:slf4j-api	1.7.7
org.slf4j:slf4j-reload4j	1.7.36
org.springframework:spring-aop	5.3.27
org.springframework:spring-beans	5.3.27
org.springframework:spring-context	5.3.27
org.springframework:spring-core	5.3.27
org.springframework:spring-expression	5.3.27
org.springframework:spring-jcl	5.3.27
org.springframework:spring-jdbc	5.3.27
org.springframework:spring-orm	5.3.27
org.springframework:spring-tx	5.3.27
org.testng:testng	7.7.1
org.tukaani:xz	1.5
org.weakref:jmxutils	1.21
org.wildfly.common:wildfly-common	1.3.0.Final
org.wildfly.security:wildfly-elytron-asn1	1.15.16.Final
org.wildfly.security:wildfly-elytron-auth-server	1.15.16.Final

org.wildfly.security:wildfly-elytron-auth	1.15.16.Final
org.wildfly.security:wildfly-elytron-base	1.15.16.Final
org.wildfly.security:wildfly-elytron-credential	1.15.16.Final
org.wildfly.security:wildfly-elytron-http	1.15.16.Final
org.wildfly.security:wildfly-elytron-keystore	1.15.16.Final
org.wildfly.security:wildfly-elytron-mechanism-digest	1.15.16.Final
org.wildfly.security:wildfly-elytron-mechanism-gssapi	1.15.16.Final
org.wildfly.security:wildfly-elytron-mechanism-oauth2	1.15.16.Final
org.wildfly.security:wildfly-elytron-mechanism-scram	1.15.16.Final
org.wildfly.security:wildfly-elytron-mechanism	1.15.16.Final
org.wildfly.security:wildfly-elytron-password-impl	1.15.16.Final
org.wildfly.security:wildfly-elytron-permission	1.15.16.Final
org.wildfly.security:wildfly-elytron-provider-util	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-digest	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-external	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-gs2	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-gssapi	1.15.1.Final
org.wildfly.security:wildfly-elytron-sasl-oauth2	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-plain	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl-scram	1.15.16.Final
org.wildfly.security:wildfly-elytron-sasl	1.15.16.Final
org.wildfly.security:wildfly-elytron-security-manager-action	1.15.16.Final
org.wildfly.security:wildfly-elytron-ssl	1.15.16.Final
org.wildfly.security:wildfly-elytron-util	1.15.16.Final
org.wildfly.security:wildfly-elytron-x500	1.15.16.Final
org.xerial.snappy:snappy-java	1.1.10.1
org.yaml:snakeyaml	2.0
software.amazon.awssdk:annotations	2.10.56
software.amazon.awssdk:annotations	2.17.128
software.amazon.awssdk:auth	2.10.56
software.amazon.awssdk:auth	2.17.128
software.amazon.awssdk:aws-cbor-protocol	2.10.56
software.amazon.awssdk:aws-core	2.10.56

software.amazon.awssdk:aws-core	2.17.128
software.amazon.awssdk:aws-json-protocol	2.10.56
software.amazon.awssdk:aws-query-protocol	2.10.56
software.amazon.awssdk:aws-query-protocol	2.17.128
software.amazon.awssdk:cloudwatch	2.10.56
software.amazon.awssdk:dynamodb	2.10.56
software.amazon.awssdk:http-client-spi	2.10.56
software.amazon.awssdk:http-client-spi	2.17.128
software.amazon.awssdk:json-utils	2.17.128
software.amazon.awssdk:kinesis	2.10.56
software.amazon.awssdk:metrics-spi	2.17.128
software.amazon.awssdk:netty-nio-client	2.10.56
software.amazon.awssdk:profiles	2.10.56
software.amazon.awssdk:profiles	2.17.128
software.amazon.awssdk:protocol-core	2.10.56
software.amazon.awssdk:protocol-core	2.17.128
software.amazon.awssdk:regions	2.10.56
software.amazon.awssdk:regions	2.17.128
software.amazon.awssdk:sdk-core	2.10.56
software.amazon.awssdk:sdk-core	2.17.128
software.amazon.awssdk:sts	2.10.56
software.amazon.awssdk:sts	2.17.128
software.amazon.awssdk:third-party-jackson-core	2.17.128
software.amazon.awssdk:utils	2.10.56
software.amazon.awssdk:utils	2.17.128
software.amazon.eventstream:eventstream	1.0.1
software.amazon.ion:ion-java	1.0.2
software.amazon.kinesis:amazon-kinesis-client	2.2.8
xmlenc:xmlenc	0.52

Vulnerabilities

ID	Description	Severity	EPSS Score	EPSS Percentile
CVE-2023-44487			0.9445	0.99992

	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.			
CVE-2024-52046	The ObjectSerializationDecoder in Apache MINA uses Java’s native deserialization protocol to process incoming serialized data but lacks the necessary security checks and defenses. This vulnerability allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to remote code execution (RCE) attacks. This issue affects MINA core versions 2.0.X, 2.1.X and 2.2.X, and will be fixed by the releases 2.0.27, 2.1.10 and 2.2.4. It's also important to note that an application using MINA core library will only be affected if the IoBuffer#getObject() method is called, and this specific method is potentially called when adding a ProtocolCodecFilter instance using the ObjectSerializationCodecFactory class in the filter chain. If your application is specifically using those classes, you have to upgrade to the latest version of MINA core library. Upgrading will not be enough: you also need to explicitly allow the classes the decoder will accept in the ObjectSerializationDecoder instance, using one of the three new methods: /** * Accept class names where the supplied ClassNameMatcher matches for * deserialization, unless they are otherwise rejected. * * @param classNameMatcher the matcher to use */ public void accept(ClassNameMatcher classNameMatcher) /** * Accept class names that match the supplied pattern for * deserialization, unless they are otherwise rejected. * * @param pattern standard Java regexp */ public void accept(Pattern pattern) /** * Accept the wildcard specified classes for deserialization, * unless they are otherwise rejected. * * @param patterns Wildcard file name patterns as defined by * {@link org.apache.commons.io.FilenameUtils#wildcardMatch(String, String) FilenameUtils.wildcardMatch} */ public void accept(String... patterns) By default, the decoder will reject *all* classes that will be present in the incoming data. Note: The FtpServer, SSHd and Vysper sub-project are not affected by this issue.		0.80138	0.99102
CVE-2023-45288	An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of header data by sending an excessive number of CONTINUATION frames. Maintaining HPACK state requires parsing and processing all HEADERS and CONTINUATION frames on a connection. When a request's headers exceed MaxHeaderBytes, no memory is allocated to store the excess headers, but they are still parsed. This permits an attacker to cause an HTTP/2 endpoint to read arbitrary amounts of header data, all associated with a request which is going to be rejected. These headers can include Huffman-encoded data which is significantly more expensive for the receiver to decode than for an attacker to send. The fix sets a limit on the amount of excess header frames we will process before closing a connection.		0.71463	0.98714
CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.		0.5673	0.98111
CVE-2024-45337	Applications and libraries which misuse connection.serverAuthenticate (via callback field ServerConfig.PublicKeyCallback) may be susceptible		0.30296	0.96651

	to an authorization bypass. The documentation for ServerConfig.PublicKeyCallback says that "A call to this function does not guarantee that the key offered is in fact used to authenticate." Specifically, the SSH protocol allows clients to inquire about whether a public key is acceptable before proving control of the corresponding private key. PublicKeyCallback may be called with multiple keys, and the order in which the keys were provided cannot be used to infer which key the client successfully authenticated with, if any. Some applications, which store the key(s) passed to PublicKeyCallback (or derived information) and make security relevant determinations based on it once the connection is established, may make incorrect assumptions. For example, an attacker may send public keys A and B, and then authenticate with A. PublicKeyCallback would be called only twice, first with A and then with B. A vulnerable application may then make authorization decisions based on key B for which the attacker does not actually control the private key. Since this API is widely misused, as a partial mitigation golang.org/x/cry...@v0.31.0 enforces the property that, when successfully authenticating via public key, the last key passed to ServerConfig.PublicKeyCallback will be the key used to authenticate the connection. PublicKeyCallback will now be called multiple times with the same key, if necessary. Note that the client may still not control the last key passed to PublicKeyCallback if the connection is then authenticated with a different method, such as PasswordCallback, KeyboardInteractiveCallback, or NoClientAuth. Users should be using the Extensions field of the Permissions return value from the various authentication callbacks to record data associated with the authentication attempt instead of referencing external state. Once the connection is established the state corresponding to the successful authentication attempt can be retrieved via the ServerConn.Permissions field. Note that some third-party libraries misuse the Permissions type by sharing it across authentication attempts; users of third-party libraries should refer to the relevant projects for guidance.			
CVE-2020-13936	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.		0.16401	0.94834
CVE-2025-27817	A possible arbitrary file read and SSRF vulnerability has been identified in Apache Kafka Client. Apache Kafka Clients accept configuration data for setting the SASL/OAUTHBEARER connection with the brokers, including "sasl.oauthbearer.token.endpoint.url" and "sasl.oauthbearer.jwks.endpoint.url". Apache Kafka allows clients to read an arbitrary file and return the content in the error log, or sending requests to an unintended location. In applications where Apache Kafka Clients configurations can be specified by an untrusted party, attackers may use the "sasl.oauthbearer.token.endpoint.url" and "sasl.oauthbearer.jwks.endpoint.url" configuratin to read arbitrary contents of the disk and environment variables or make requests to an unintended location. In particular, this flaw may be used in Apache Kafka Connect to escalate from REST API access to filesystem/ environment/URL access, which may be undesirable in certain environments, including SaaS products. Since Apache Kafka 3.9.1/4.0.0, we have added a system property ("-Dorg.apache.kafka.sasl.oauthbearer.allowed.urls") to set the allowed urls in SASL JAAS configuration. In 3.9.1, it accepts all urls by default for backward compatibility. However in 4.0.0 and newer, the default value is empty list and users have to set the allowed urls explicitly.		0.13418	0.94153
CVE-2019-10202	A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.		0.0724	0.91582
CVE-2024-28180	Package jose aims to provide an implementation of the Javascript Object Signing and Encryption set of standards. An attacker could send a JWE containing compressed data that used large amounts of memory and CPU when decompressed by Decrypt or DecryptMulti. Those functions now return an error if the decompressed data would exceed 250kB or 10x the compressed size (whichever is larger). This vulnerability has been patched in versions 4.0.1, 3.0.3 and 2.6.3.		0.04859	0.89509
CVE-2023-40167	Jetty is a Java based web server and servlet engine. Prior to versions 9.4.52, 10.0.16, 11.0.16, and 12.0.1, Jetty accepts the `+` character proceeding the content-length value in a HTTP/1 header field. This is more permissive than allowed by the RFC and other servers routinely reject such requests with 400 responses. There is no known exploit scenario, but it is conceivable that request smuggling could result if		0.04833	0.8948

	jetty is used in combination with a server that does not close the connection after sending such a 400 response. Versions 9.4.52, 10.0.16, 11.0.16, and 12.0.1 contain a patch for this issue. There is no workaround as there is no known exploit scenario.			
CVE-2022-31197	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue.		0.03579	0.87686
CVE-2023-22102	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.1.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Connectors, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).		0.03493	0.87539
CVE-2021-42550	In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.		0.02729	0.85885
CVE-2022-28948	An issue in the Unmarshal function in Go-Yaml v3 causes the program to crash when attempting to deserialize invalid input.		0.01524	0.81208
CVE-2024-8184	There exists a security vulnerability in Jetty's ThreadLimitHandler.getRemote() which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory.		0.01487	0.80973
CVE-2024-38820	The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.		0.01473	0.80882
CVE-2023-36478	Eclipse Jetty provides a web server and servlet container. In versions 11.0.0 through 11.0.15, 10.0.0 through 10.0.15, and 9.0.0 through 9.4.52, an integer overflow in `MetaDataBuilder.checkSize` allows for HTTP/2 HPACK header values to exceed their size limit. `MetaDataBuilder.java` determines if a header name or value exceeds the size limit, and throws an exception if the limit is exceeded. However, when length is very large and huffman is true, the multiplication by 4 in line 295 will overflow, and length will become negative. `(_size+length)` will now be negative, and the check on line 296 will not be triggered. Furthermore, `MetaDataBuilder.checkSize` allows for user-entered HPACK header value sizes to be negative, potentially leading to a very large buffer allocation later on when the user-entered size is multiplied by 2. This means that if a user provides a negative length value (or, more precisely, a length value which, when multiplied by the 4/3 fudge factor, is negative), and this length value is a very large positive number when multiplied by 2, then the user can cause a very large buffer to be allocated on the server. Users of HTTP/2 can be impacted by a remote denial of service attack. The issue has been fixed in versions 11.0.16, 10.0.16, and 9.4.53. There are no known workarounds.		0.01459	0.80777

CVE-2023-36479	Eclipse Jetty Canonical Repository is the canonical repository for the Jetty project. Users of the CgiServlet with a very specific command structure may have the wrong command executed. If a user sends a request to a org.eclipse.jetty.servlets.CGI Servlet for a binary with a space in its name, the servlet will escape the command by wrapping it in quotation marks. This wrapped command, plus an optional command prefix, will then be executed through a call to Runtime.exec. If the original binary name provided by the user contains a quotation mark followed by a space, the resulting command line will contain multiple tokens instead of one. This issue was patched in version 9.4.52, 10.0.16, 11.0.16 and 12.0.0-beta2.		0.01383	0.80248
CVE-2021-0341	In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171980069		0.01037	0.77343
CVE-2024-6763	Eclipse Jetty is a lightweight, highly scalable, Java-based web server and Servlet engine . It includes a utility class, HttpURI, for URI/URL parsing. The HttpURI class does insufficient validation on the authority segment of a URI. However the behaviour of HttpURI differs from the common browsers in how it handles a URI that would be considered invalid if fully validated against the RRC. Specifically HttpURI and the browser may differ on the value of the host extracted from an invalid URI and thus a combination of Jetty and a vulnerable browser may be vulnerable to a open redirect attack or to a SSRF attack if the URI is used after passing validation checks.		0.01022	0.77184
CVE-2023-46120	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0.		0.01	0.76916
CVE-2025-24970	Netty, an asynchronous, event-driven network application framework, has a vulnerability starting in version 4.1.91.Final and prior to version 4.1.118.Final. When a special crafted packet is received via SslHandler it doesn't correctly handle validation of such a packet in all cases which can lead to a native crash. Version 4.1.118.Final contains a patch. As workaround its possible to either disable the usage of the native SSLEngine or change the code manually.		0.0098	0.76704
CVE-2021-41973	In Apache MINA, a specifically crafted, malformed HTTP request may cause the HTTP Header decoder to loop indefinitely. The decoder assumed that the HTTP Header begins at the beginning of the buffer and loops if there is more data than expected. Please update MINA to 2.1.5 or greater.		0.0084	0.74666
CVE-2024-38808	In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) expression that may cause a denial of service (DoS) condition. Specifically, an application is vulnerable when the following is true: * The application evaluates user-supplied SpEL expressions.		0.00809	0.74164
CVE-2018-1313	In Apache Derby 10.3.1.4 to 10.14.1.0, a specially-crafted network packet can be used to request the Derby Network Server to boot a database whose location and contents are under the user's control. If the Derby Network Server is not running with a Java Security Manager policy file, the attack is successful. If the server is using a policy file, the policy file must permit the database location to be read for the attack to work. The default Derby Network Server policy file distributed with the affected releases includes a permissive policy as the default Network Server policy, which allows the attack to work.		0.00772	0.73506
CVE-2025-46392	Uncontrolled Resource Consumption vulnerability in Apache Commons Configuration 1.x. There are a number of issues in Apache Commons Configuration 1.x that allow excessive resource consumption when loading untrusted configurations or using unexpected usage patterns. The Apache Commons Configuration team does not intend to fix these issues in 1.x. Apache Commons Configuration 1.x is still safe to use in scenario's where you only load trusted configurations. Users that load untrusted configurations or give attackers control over usage patterns are recommended to upgrade to the 2.x version line, which fixes these issues. Apache Commons Configuration 2.x is not a drop-in		0.00762	0.73309

	replacement, but as it uses a separate Maven groupId and Java package namespace they can be loaded side-by-side, making it possible to do a gradual migration.			
CVE-2024-47561	Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code. Users are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue.		0.00747	0.73022
CVE-2024-29133	Out-of-bounds Write vulnerability in Apache Commons Configuration.This issue affects Apache Commons Configuration: from 2.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1, which fixes the issue.		0.00737	0.72772
CVE-2020-13949	In Apache Thrift 0.9.3 to 0.13.0, malicious RPC clients could send short messages which would result in a large memory allocation, potentially leading to denial of service.		0.00731	0.72624
CVE-2019-0231	Handling of the close_notify SSL/TLS message does not lead to a connection closure, leading the server to retain the socket opened and to have the client potentially receive clear text messages afterward. Mitigation: 2.0.20 users should migrate to 2.0.21, 2.1.0 users should migrate to 2.1.1. This issue affects: Apache MINA.		0.00726	0.72544
CVE-2019-0205	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.		0.00698	0.71917
CVE-2024-9823	There exists a security vulnerability in Jetty's DosFilter which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack on the server using DosFilter. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory finally.		0.0068	0.71537
CVE-2023-6378	A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.		0.00613	0.69768
CVE-2023-7272	In Eclipse Parsson before 1.0.4 and 1.1.3, a document with a large depth of nested objects can allow an attacker to cause a Java stack overflow exception and denial of service. Eclipse Parsson allows processing (e.g. parse, generate, transform and query) JSON documents.		0.00566	0.68394
CVE-2019-10172	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.		0.00563	0.68279
CVE-2024-22201	Jetty is a Java based web server and servlet engine. An HTTP/2 SSL connection that is established and TCP congested will be leaked when it times out. An attacker can cause many connections to end up in this state, and the server may run out of file descriptors, eventually causing the server to stop accepting new connections from valid clients. The vulnerability is patched in 9.4.54, 10.0.20, 11.0.20, and 12.0.6.		0.00559	0.68169
CVE-2024-13009	In Eclipse Jetty versions 9.4.0 to 9.4.56 a buffer can be incorrectly released when confronted with a gzip error when inflating a request body. This can result in corrupted and/or inadvertent sharing of data between requests.		0.00554	0.67999
CVE-2018-11798	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.		0.00546	0.6776
CVE-2023-5384	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the credentials are returned in clear text as part of the configuration.		0.00527	0.66969
CVE-2023-3635	GzipSource does not handle an exception that might be raised when parsing a malformed gzip buffer. This may lead to denial of service of the Okio client when handling a crafted GZIP archive, by using the GzipSource class.		0.00498	0.6579

CVE-2024-1597	pgjdbc, the PostgreSQL JDBC Driver, allows attacker to inject SQL if using PreferQueryMode=SIMPLE. Note this is not the default. In the default mode there is no vulnerability. A placeholder for a numeric value must be immediately preceded by a minus. There must be a second placeholder for a string value after the first placeholder; both must be on the same line. By constructing a matching string payload, the attacker can inject SQL to alter the query,bypassing the protections that parameterized queries bring against SQL Injection attacks. Versions before 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9, and 42.2.28 are affected.		0.00476	0.64775
CVE-2024-47535	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes. This vulnerability is fixed in 4.1.115.		0.00467	0.64366
CVE-2024-21634	Amazon Ion is a Java implementation of the Ion data notation. Prior to version 1.10.5, a potential denial-of-service issue exists in `ion-java` for applications that use `ion-java` to deserialize Ion text encoded data, or deserialize Ion text or binary encoded data into the `IonValue` model and then invoke certain `IonValue` methods on that in-memory representation. An actor could craft Ion data that, when loaded by the affected application and/or processed using the `IonValue` model, results in a `StackOverflowError` originating from the `ion-java` library. The patch is included in `ion-java` 1.10.5. As a workaround, do not load data which originated from an untrusted source or that could have been tampered with.		0.00458	0.63916
CVE-2023-29408	The TIFF decoder does not place a limit on the size of compressed tile data. A maliciously-crafted image can exploit this to cause a small image (both in terms of pixel width/height, and encoded size) to make the decoder decode large amounts of compressed data, consuming excessive memory and CPU.		0.00433	0.6261
CVE-2023-51775	The jose4j component before 0.9.4 for Java allows attackers to cause a denial of service (CPU consumption) via a large p2c (aka PBES2 Count) value.		0.00429	0.62384
CVE-2024-26308	Allocation of Resources Without Limits or Throttling vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.21 before 1.26. Users are recommended to upgrade to version 1.26, which fixes the issue.		0.00392	0.60097
CVE-2022-41717	An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys can cause the server to allocate approximately 64 MiB per open connection.		0.00331	0.55902
CVE-2024-53990	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. When making any HTTP request, the automatically enabled and self-managed CookieStore (aka cookie jar) will silently replace explicitly defined Cookies with any that have the same name from the cookie jar. For services that operate with multiple users, this can result in one user's Cookie being used for another user's requests.		0.00325	0.55368
CVE-2023-43642	snappy-java is a Java port of the snappy, a fast C++ compresser/ decompresser developed by Google. The SnappyInputStream was found to be vulnerable to Denial of Service (DoS) attacks when decompressing data with a too large chunk size. Due to missing upper bound check on chunk length, an unrecoverable fatal error can occur. All versions of snappy-java including the latest released version 1.1.10.3 are vulnerable to this issue. A fix has been introduced in commit `9f8c3cf74` which will be included in the 1.1.10.4 release. Users are advised to upgrade. Users unable to upgrade should only accept compressed data from trusted sources.		0.00322	0.55174
CVE-2024-24786	The protojson.Unmarshal function can enter an infinite loop when unmarshaling certain forms of invalid JSON. This condition can occur when unmarshaling into a message which contains a google.protobuf.Any value, or when the UnmarshalOptions.DiscardUnknown option is set.		0.00322	0.55166
CVE-2019-19794	The miekg Go DNS package before 1.1.25, as used in CoreDNS before 1.6.6 and other products, improperly generates random numbers		0.00297	0.53034

	because math/rand is used. The TXID becomes predictable, leading to response forgeries.			
CVE-2025-59419	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.128.Final and 4.2.7.Final, the SMTP codec in Netty contains an SMTP command injection vulnerability due to insufficient input validation for Carriage Return (\r) and Line Feed (\n) characters in user-supplied parameters. The vulnerability exists in io.netty.handler.codec.smtp.DefaultSmtpRequest, where parameters are directly concatenated into the SMTP command string without sanitization. When methods such as SmtpRequests.rcpt(recipient) are called with a malicious string containing CRLF sequences, attackers can inject arbitrary SMTP commands. Because the injected commands are sent from the server's trusted IP address, resulting emails will likely pass SPF and DKIM authentication checks, making them appear legitimate. This allows remote attackers who can control SMTP command parameters (such as email recipients) to forge arbitrary emails from the trusted server, potentially impersonating executives and forging high-stakes corporate communications. This issue has been patched in versions 4.1.129.Final and 4.2.8.Final. No known workarounds exist.		0.00295	0.52757
CVE-2022-41723	A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.		0.00272	0.50584
CVE-2024-29025	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `HttpPostRequestDecoder` can be tricked to accumulate data. While the decoder can store items on the disk if configured so, there are no limits to the number of fields the form can have, an attacher can send a chunked post consisting of many small fields that will be accumulated in the `bodyListHttpData` list. The decoder cumulates bytes in the `undecodedChunk` buffer until it can decode a field, this field can cumulate data without limits. This vulnerability is fixed in 4.1.108.Final.		0.00268	0.50214
CVE-2021-37533	Prior to Apache Commons Net 3.9.0, Net's FTP client trusts the host from PASV response by default. A malicious server can redirect the Commons Net code to use a different host, but the user has to connect to the malicious server in the first place. This may lead to leakage of information about services running on the private network of the client. The default in version 3.9.0 is now false to ignore such hosts, as cURL does. See https://issues.apache.org/jira/browse/NET-711.		0.00249	0.48115
CVE-2023-29407	A maliciously-crafted image can cause excessive CPU consumption in decoding. A tiled image with a height of 0 and a very large width can cause excessive CPU consumption, despite the image size (width * height) appearing to be zero.		0.00241	0.4727
CVE-2025-22869	SSH servers which implement file transfer protocols are vulnerable to a denial of service attack from clients which complete the key exchange slowly, or not at all, causing pending content to be read into memory, but never transmitted.		0.00215	0.43963
CVE-2020-8911	A padding oracle vulnerability exists in the AWS S3 Crypto SDK for GoLang versions prior to V2. The SDK allows users to encrypt files with AES-CBC without computing a Message Authentication Code (MAC), which then allows an attacker who has write access to the target's S3 bucket and can observe whether or not an endpoint with access to the key can decrypt a file, they can reconstruct the plaintext with (on average) 128*length (plaintext) queries to the endpoint, by exploiting CBC's ability to manipulate the bytes of the next block and PKCS5 padding errors. It is recommended to update your SDK to V2 or later, and re-encrypt your files.		0.00203	0.42368
CVE-2024-29857	An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before 1.78, BC Java LTS before 2.73.6, BC-FJA before 1.0.2.5, and BC C# .Net before 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.		0.00191	0.40917
CVE-2024-25638	dnsjava is an implementation of DNS in Java. Records in DNS replies are not checked for their relevance to the query, allowing an attacker to respond with RRs from different zones. This vulnerability is fixed in 3.6.0.		0.00188	0.40621
CVE-2025-48734			0.00186	0.40323

	Improper Access Control vulnerability in Apache Commons. A special BeanIntrospector class was added in version 1.9.2. This can be used to stop attackers from using the declared class property of Java enum objects to get access to the classloader. However this protection was not enabled by default. PropertyUtilsBean (and consequently BeanUtilsBean) now disallows declared class level property access by default. Releases 1.11.0 and 2.0.0-M2 address a potential security issue when accessing enum properties in an uncontrolled way. If an application using Commons BeanUtils passes property paths from an external source directly to the getProperty() method of PropertyUtilsBean, an attacker can access the enum's class loader via the "declaredClass" property available on all Java "enum" objects. Accessing the enum's "declaredClass" allows remote attackers to access the ClassLoader and execute arbitrary code. The same issue exists with PropertyUtilsBean.getNestedProperty(). Starting in versions 1.11.0 and 2.0.0-M2 a special BeanIntrospector suppresses the "declaredClass" property. Note that this new BeanIntrospector is enabled by default, but you can disable it to regain the old behavior; see section 2.5 of the user's guide and the unit tests. This issue affects Apache Commons BeanUtils 1.x before 1.11.0, and 2.x before 2.0.0-M2.Users of the artifact commons-beanutils:commons-beanutils 1.x are recommended to upgrade to version 1.11.0, which fixes the issue. Users of the artifact org.apache.commons:commons-beanutils2 2.x are recommended to upgrade to version 2.0.0-M2, which fixes the issue.			
CVE-2024-29131	Out-of-bounds Write vulnerability in Apache Commons Configuration.This issue affects Apache Commons Configuration: from 2.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1, which fixes the issue.		0.00183	0.39929
CVE-2022-29526	Go before 1.17.10 and 1.18.x before 1.18.2 has Incorrect Privilege Assignment. When called with a non-zero flags parameter, the Faccessat function could incorrectly report that a file is accessible.		0.00182	0.39851
CVE-2024-1300	A vulnerability in the Eclipse Vert.x toolkit causes a memory leak in TCP servers configured with TLS and SNI support. When processing an unknown SNI server name assigned the default certificate instead of a mapped certificate, the SSL context is erroneously cached in the server name map, leading to memory exhaustion. This flaw allows attackers to send TLS client hello messages with fake server names, triggering a JVM out-of-memory error.		0.00181	0.39604
CVE-2024-47554	Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.		0.00173	0.38554
CVE-2024-24792	Parsing a corrupt or malicious image with invalid color indices can cause a panic.		0.00162	0.37003
CVE-2023-39325	A malicious HTTP/2 client which rapidly creates requests and immediately resets them can cause excessive server resource consumption. While the total number of requests is bounded by the http2.Server.MaxConcurrentStreams setting, resetting an in-progress request allows the attacker to create a new request while the existing one is still executing. With the fix applied, HTTP/2 servers now bound the number of simultaneously executing handler goroutines to the stream concurrency limit (MaxConcurrentStreams). New requests arriving when at the limit (which can only happen after the client has reset an existing, in-flight request) will be queued until a handler exits. If the request queue grows too large, the server will terminate the connection. This issue is also fixed in golang.org/x/net/http2 for users manually configuring HTTP/2. The default stream concurrency limit is 250 streams (requests) per HTTP/2 connection. This value may be adjusted using the golang.org/x/net/http2 package; see the Server.MaxConcurrentStreams setting and the ConfigureServer function.		0.0015	0.3538
CVE-2020-8912	A vulnerability in the in-band key negotiation exists in the AWS S3 Crypto SDK for GoLang versions prior to V2. An attacker with write access to the targeted bucket can change the encryption algorithm of an object in the bucket, which can then allow them to change AES-GCM to AES-CTR. Using this in combination with a decryption oracle can reveal the authentication key used by AES-GCM as decrypting the GMAC tag leaves the authentication key recoverable as an algebraic equation. It is recommended to update your SDK to V2 or later, and re-encrypt your files.		0.00141	0.34005

CVE-2022-41946	pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.		0.00126	0.31886
CVE-2023-1419	A script injection vulnerability was found in the Debezium database connector, where it does not properly sanitize some parameters. This flaw allows an attacker to send a malicious request to inject a parameter that may allow the viewing of unauthorized data.		0.00126	0.31816
CVE-2025-5115	In Eclipse Jetty, versions <=9.4.57, <=10.0.25, <=11.0.25, <=12.0.21, <=12.1.0.alpha2, an HTTP/2 client may trigger the server to send RST_STREAM frames, for example by sending frames that are malformed or that should not be sent in a particular stream state, therefore forcing the server to consume resources such as CPU and memory. For example, a client can open a stream and then send WINDOW_UPDATE frames with window size increment of 0, which is illegal. Per specification https://www.rfc-editor.org/rfc/rfc9113.html#name-window_update , the server should send a RST_STREAM frame. The client can now open another stream and send another bad WINDOW_UPDATE, therefore causing the server to consume more resources than necessary, as this case does not exceed the max number of concurrent streams, yet the client is able to create an enormous amount of streams in a short period of time. The attack can be performed with other conditions (for example, a DATA frame for a closed stream) that cause the server to send a RST_STREAM frame. Links: * https://github.com/jetty/jetty.project/security/advisories/GHSA-mmxm-8w33-wc4h		0.00125	0.31712
CVE-2022-45146	An issue was discovered in the FIPS Java API of Bouncy Castle BC-FJA before 1.0.2.4. Changes to the JVM garbage collector in Java 13 and later trigger an issue in the BC-FJA FIPS modules where it is possible for temporary keys used by the module to be zeroed out while still in use by the module, resulting in errors or potential information loss. NOTE: FIPS compliant users are unaffected because the FIPS certification is only for Java 7, 8, and 11.		0.00124	0.31604
CVE-2018-1320	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.		0.00121	0.3103
CVE-2024-36114	Aircompressor is a library with ports of the Snappy, LZO, LZ4, and Zstandard compression algorithms to Java. All decompressor implementations of Aircompressor (LZ4, LZO, Snappy, Zstandard) can crash the JVM for certain input, and in some cases also leak the content of other memory of the Java process (which could contain sensitive information). When decompressing certain data, the decompressors try to access memory outside the bounds of the given byte arrays or byte buffers. Because Aircompressor uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. Users should update to Aircompressor 0.27 or newer where these issues have been fixed. When decompressing data from untrusted users, this can be exploited for a denial-of-service attack by crashing the JVM, or to leak other sensitive information from the Java process. There are no known workarounds for this issue.		0.0012	0.30993
CVE-2025-22872	The tokenizer incorrectly interprets tags with unquoted attribute values that end with a solidus character (/) as self-closing. When directly using Tokenizer, this can result in such tags incorrectly being marked as self-closing, and when using the Parse functions, this can result in content following such tags as being placed in the wrong scope during DOM		0.00119	0.30813

	construction, but only when tags are in foreign content (e.g. <math>, <svg>, etc contexts).			
CVE-2024-31141	Files or Directories Accessible to External Parties, Improper Privilege Management vulnerability in Apache Kafka Clients. Apache Kafka Clients accept configuration data for customizing behavior, and includes ConfigProvider plugins in order to manipulate these configurations. Apache Kafka also provides FileConfigProvider, DirectoryConfigProvider, and EnvVarConfigProvider implementations which include the ability to read from disk or environment variables. In applications where Apache Kafka Clients configurations can be specified by an untrusted party, attackers may use these ConfigProviders to read arbitrary contents of the disk and environment variables. In particular, this flaw may be used in Apache Kafka Connect to escalate from REST API access to filesystem/environment access, which may be undesirable in certain environments, including SaaS products. This issue affects Apache Kafka Clients: from 2.3.0 through 3.5.2, 3.6.2, 3.7.0. Users with affected applications are recommended to upgrade kafka-clients to version >=3.8.0, and set the JVM system property "org.apache.kafka.automatic.config.providers=none". Users of Kafka Connect with one of the listed ConfigProvider implementations specified in their worker config are also recommended to add appropriate "allowlist.pattern" and "allowed.paths" to restrict their operation to appropriate bounds. For users of Kafka Clients or Kafka Connect in environments that trust users with disk and environment variable access, it is not recommended to set the system property. For users of the Kafka Broker, Kafka MirrorMaker 2.0, Kafka Streams, and Kafka command-line tools, it is not recommended to set the system property.		0.00115	0.30166
CVE-2022-2582	The AWS S3 Crypto SDK sends an unencrypted hash of the plaintext alongside the ciphertext as a metadata field. This hash can be used to brute force the plaintext, if the hash is readable to the attacker. AWS now blocks this metadata field, but older SDK versions still send it.		0.00113	0.29886
CVE-2025-22868	An attacker can pass a malicious malformed token which causes unexpected memory to be consumed during parsing.		0.00112	0.29739
CVE-2024-34447	An issue was discovered in the Bouncy Castle Crypto Package For Java before BC TLS Java 1.0.19 (ships with BC Java 1.78, BC Java (LTS) 2.73.6) and before BC FIPS TLS Java 1.0.19. When endpoint identification is enabled in the BCJSSE and an SSL socket is created without an explicit hostname (as happens with HttpsURLConnection), hostname verification could be performed against a DNS-resolved IP address in some situations, opening up a possibility of DNS poisoning.		0.00107	0.28888
CVE-2023-52428	In Connect2id Nimbus JOSE+JWT before 9.37.2, an attacker can cause a denial of service (resource consumption) via a large JWE p2c header value (aka iteration count) for the PasswordBasedDecrypter (PBKDF2) component.		0.00105	0.28642
CVE-2024-30171	An issue was discovered in Bouncy Castle Java TLS API and JSSE Provider before 1.78. Timing-based leakage may occur in RSA based handshakes because of exception processing.		0.00105	0.28596
CVE-2024-23454	Apache Hadoop’s RunJar.run() does not set permissions for temporary directory by default. If sensitive data will be present in this file, all the other local users may be able to view the content. This is because, on unix-like systems, the system temporary directory is shared between all local users. As such, files written in this directory, without setting the correct posix permissions explicitly, may be viewable by all other local users.		0.00104	0.28376
CVE-2025-30204	golang-jwt is a Go implementation of JSON Web Tokens. Starting in version 3.2.0 and prior to versions 5.2.2 and 4.5.2, the function parse.ParseUnverified splits (via a call to strings.Split) its argument (which is untrusted data) on periods. As a result, in the face of a malicious request whose Authorization header consists of Bearer followed by many period characters, a call to that function incurs allocations to the tune of O(n) bytes (where n stands for the length of the function's argument), with a constant factor of about 16. This issue is fixed in 5.2.2 and 4.5.2.		0.00102	0.2809
CVE-2022-27664	In net/http in Go before 1.18.6 and 1.19.x before 1.19.1, attackers can cause a denial of service because an HTTP/2 connection can hang during closing if shutdown were preempted by a fatal error.		0.00101	0.27877
CVE-2023-5236	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with		0.001	0.27831

	sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service.			
CVE-2025-25193	Netty, an asynchronous, event-driven network application framework, has a vulnerability in versions up to and including 4.1.118.Final. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crash. A similar issue was previously reported as CVE-2024-47535. This issue was fixed, but the fix was incomplete in that null-bytes were not counted against the input limit. Commit d1fbda62d3a47835d3fb35db8bd42ecc205a5386 contains an updated fix.		0.00098	0.27114
CVE-2023-3978	Text nodes not in the HTML namespace are incorrectly literally rendered, causing text which should be escaped to not be. This could lead to an XSS attack.		0.00097	0.26902
CVE-2025-11143	The Jetty URI parser has some key differences to other common parsers when evaluating invalid or unusual URIs. Differential parsing of URIs in systems using multiple components may result in security by-pass. For example a component that enforces a black list may interpret the URIs differently from one that generates a response. At the very least, differential parsing may divulge implementation details.		0.00093	0.26124
CVE-2022-27191	The golang.org/x/crypto/ssh package before 0.0.0-20220314234659-1baeb1ce4c0b for Go allows an attacker to crash a server in certain circumstances involving AddHostKey.		0.00089	0.25379
CVE-2024-12798	ACE vulnerability in JaninoEventEvaluator by QOS.CH logback-core upto including version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 in Java applications allows attacker to execute arbitrary code by compromising an existing logback configuration file or by injecting an environment variable before program execution. Malicious logback configuration files can allow the attacker to execute arbitrary code using the JaninoEventEvaluator extension. A successful attack requires the user to have write access to a configuration file. Alternatively, the attacker could inject a malicious environment variable pointing to a malicious configuration file. In both cases, the attack requires existing privilege.		0.00089	0.25374
CVE-2025-58181	SSH servers parsing GSSAPI authentication requests do not validate the number of mechanisms specified in the request, allowing an attacker to cause unbounded memory consumption.		0.00087	0.25082
CVE-2025-22233	CVE-2024-38820 ensured Locale-independent, lowercase conversion for both the configured disallowedFields patterns and for request parameter names. However, there are still cases where it is possible to bypass the disallowedFields checks. Affected Spring Products and Versions Spring Framework: * 6.2.0 - 6.2.6 * 6.1.0 - 6.1.19 * 6.0.0 - 6.0.27 * 5.3.0 - 5.3.42 * Older, unsupported versions are also affected Mitigation Users of affected versions should upgrade to the corresponding fixed version. Affected version(s)Fix Version Availability 6.2.x 6.2.7 OSS6.1.x 6.1.20 OSS6.0.x 6.0.28 Commercial https://enterprise.spring.io/ 5.3.x 5.3.43 Commercial https://enterprise.spring.io/ No further mitigation steps are necessary. Generally, we recommend using a dedicated model object with properties only for data binding, or using constructor binding since constructor arguments explicitly declare what to bind together with turning off setter binding through the declarativeBinding flag. See the Model Design section in the reference documentation. For setting binding, prefer the use of allowedFields (an explicit list) over disallowedFields. Credit This issue was responsibly reported by the TERASOLUNA Framework Development Team from NTT DATA Group Corporation.		0.00083	0.24221
CVE-2024-45339	When logs are written to a widely-writable directory (the default), an unprivileged attacker may predict a privileged process's log file path and pre-create a symbolic link to a sensitive file in its place. When that privileged process runs, it will follow the planted symlink and overwrite that sensitive file. To fix that, glog now causes the program to exit (with status code 2) when it finds that the configured log file already exists.		0.00079	0.23302
CVE-2025-52999	jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. In versions prior to 2.15.0, if a user parses an input file and it has deeply nested data, Jackson could end up throwing a StackoverflowError if the depth is particularly large. jackson-core 2.15.0 contains a configurable limit for how deep Jackson will traverse in an input document, defaulting to an		0.00078	0.23262

	allowable depth of 1000. jackson-core will throw a StreamConstraintsException if the limit is reached. jackson-databind also benefits from this change because it uses jackson-core to parse JSON inputs. As a workaround, users should avoid parsing input files from untrusted sources.			
CVE-2024-30172	An issue was discovered in Bouncy Castle Java Cryptography APIs before 1.78. An Ed25519 verification code infinite loop can occur via a crafted signature and public key.		0.00077	0.22972
CVE-2024-7254	Any project that parses untrusted Protocol Buffers data containing an arbitrary number of nested groups / series of SGROUP tags can corrupted by exceeding the stack limit i.e. StackOverflow. Parsing nested groups as unknown fields with DiscardUnknownFieldsParser or Java Protobuf Lite parser, or against Protobuf map fields, creates unbounded recursions that can be abused by an attacker.		0.00077	0.22828
CVE-2025-59250	Improper input validation in JDBC Driver for SQL Server allows an unauthorized attacker to perform spoofing over a network.		0.00077	0.22836
CVE-2025-8885	Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. BC Java bcprov on All (API modules), Legion of the Bouncy Castle Inc. BC-FJA bc-fips on All allows Excessive Allocation. This vulnerability is associated with program files https://github.com/bcgit/bc-java/blob/main/core/src/main/java/org/bouncycastle/asn1/ASN1ObjectIdenti... https://github.com/bcgit/bc-java/blob/main/core/src/main/java/org/bouncycastle/asn1/ASN1ObjectIdentifier.Java . This issue affects BC Java: from 1.0 through 1.77; BC-FJA: from 1.0.0 through 1.0.2.5, from 2.0.0 through 2.0.1.		0.00071	0.21572
CVE-2025-58057	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In netty-codec-compression versions 4.1.124.Final and below, and netty-codec versions 4.2.4.Final and below, when supplied with specially crafted input, BrotliDecoder and certain other decompression decoders will allocate a large number of reachable byte buffers, which can lead to denial of service. BrotliDecoder.decompress has no limit in how often it calls pull, decompressing data 64K bytes at a time. The buffers are saved in the output list, and remain reachable until OOM is hit. This is fixed in versions 4.1.125.Final of netty-codec and 4.2.5.Final of netty-codec-compression.		0.00065	0.20249
CVE-2025-41249	The Spring Framework annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue if such annotations are used for authorization decisions. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE is published in conjunction with CVE-2025-41248 https://spring.io/security/cve-2025-41248 .		0.00064	0.20014
CVE-2025-63811	An issue was discovered in dvsekhvalnov jose2go 1.5.0 thru 1.7.0 allowing an attacker to cause a Denial-of-Service (DoS) via crafted JSON Web Encryption (JWE) token with an exceptionally high compression ratio.		0.00064	0.20025
CVE-2026-33871	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, a remote user can trigger a Denial of Service (DoS) against a Netty HTTP/2 server by sending a flood of `CONTINUATION` frames. The server's lack of a limit on the number of `CONTINUATION` frames, combined with a bypass of existing size-based mitigations using zero-byte frames, allows an user to cause excessive CPU consumption with minimal bandwidth, rendering the server unresponsive. Versions 4.1.132.Final and 4.2.10.Final fix the issue.		0.00062	0.19295
CVE-2023-39410	When deserializing untrusted or corrupted data, it is possible for a reader to consume memory beyond the allowed constraints and thus lead to out of memory on the system. This issue affects Java applications using Apache Avro Java SDK up to and including 1.11.2. Users should update to apache-avro version 1.11.3 which addresses this issue.		0.00061	0.1904
CVE-2025-11226	ACE vulnerability in conditional configuration file processing by QOS.CH logback-core up to and including version 1.5.18 in Java applications, allows an attacker to execute arbitrary code by compromising an		0.00058	0.18063

	existing logback configuration file or by injecting an environment variable before program execution. A successful attack requires the presence of Janino library and Spring Framework to be present on the user's class path. In addition, the attacker must have write access to a configuration file. Alternatively, the attacker could inject a malicious environment variable pointing to a malicious configuration file. In both cases, the attack requires existing privilege.			
CVE-2022-32149	An attacker may cause a denial of service by crafting an Accept-Language header which ParseAcceptLanguage will take significant time to parse.		0.00054	0.16943
CVE-2023-50658	The jose2go component before 1.6.0 for Go allows attackers to cause a denial of service (CPU consumption) via a large p2c (aka PBES2 Count) value.		0.00054	0.16893
CVE-2021-38561	golang.org/x/text/language in golang.org/x/text before 0.3.7 can panic with an out-of-bounds read during BCP 47 language tag parsing. Index calculation is mishandled. If parsing untrusted user input, this can be used as a vector for a denial-of-service attack.		0.00053	0.16562
CVE-2025-67721	Aircompressor is a library with ports of the Snappy, LZO, LZ4, and Zstandard compression algorithms to Java. In versions 3.3 and below, incorrect handling of malformed data in Java-based decompressor implementations for Snappy and LZ4 allow remote attackers to read previous buffer contents via crafted compressed input. With certain crafted compressed inputs, elements from the output buffer can end up in the uncompressed output, potentially leaking sensitive data. This is relevant for applications that reuse the same output buffer to uncompress multiple inputs. This can be the case of a web server that allocates a fix-sized buffer for performance purposes. There is similar vulnerability in GHSA-cmp6-m4wj-q63q. This issue is fixed in version 3.4.		0.00053	0.16571
CVE-2025-53864	Connect2id Nimbus JOSE + JWT 10.0.x before 10.0.2 and 9.37.x before 9.37.4 allows a remote attacker to cause a denial of service via a deeply nested JSON object supplied in a JWT claim set, because of uncontrolled recursion. NOTE: this is independent of the Gson 2.11.0 issue because the Connect2id product could have checked the JSON object nesting depth, regardless of what limits (if any) were imposed by Gson.		0.00049	0.15086
CVE-2025-11965	In Eclipse Vert.x versions [4.0.0, 4.5.21] and [5.0.0, 5.0.4], a StaticHandler configuration for restricting access to hidden files fails to restrict access to hidden directories, allowing unauthorized users to retrieve files within them (e.g. '.git/config').		0.00048	0.14756
CVE-2022-46337	A cleverly devised username might bypass LDAP authentication checks. In LDAP-authenticated Derby installations, this could let an attacker fill up the disk by creating junk Derby databases. In LDAP-authenticated Derby installations, this could also allow the attacker to execute malware which was visible to and executable by the account which booted the Derby server. In LDAP-protected databases which weren't also protected by SQL GRANT/REVOKE authorization, this vulnerability could also let an attacker view and corrupt sensitive data and run sensitive database functions and procedures. Mitigation: Users should upgrade to Java 21 and Derby 10.17.1.0. Alternatively, users who wish to remain on older Java versions should build their own Derby distribution from one of the release families to which the fix was backported: 10.16, 10.15, and 10.14. Those are the releases which correspond, respectively, with Java LTS versions 17, 11, and 8.		0.00047	0.14378
CVE-2024-12801	Server-Side Request Forgery (SSRF) in SaxEventRecorder by QOS.CH logback version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 on the Java platform, allows an attacker to forge requests by compromising logback configuration files in XML. The attacks involves the modification of DOCTYPE declaration in XML configuration files.		0.00046	0.14049
CVE-2023-50298	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr.This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. Solr Streaming Expressions allows users to extract data from other Solr Clouds, using a "zkHost" parameter. When original SolrCloud is setup to use ZooKeeper credentials and ACLs, they will be sent to whatever "zkHost" the user provides. An attacker could setup a server to mock ZooKeeper, that accepts ZooKeeper requests with credentials and ACLs and extracts the sensitive information, then send a streaming expression using the mock server's address in "zkHost". Streaming Expressions are exposed via the "/streaming" handler, with "read" permissions. Users are recommended to upgrade		0.00045	0.13696

	to version 8.11.3 or 9.4.1, which fix the issue. From these versions on, only zkHost values that have the same server address (regardless of chroot), will use the given ZooKeeper credentials and ACLs when connecting.			
CVE-2025-58056	Netty is an asynchronous event-driven network application framework for development of maintainable high performance protocol servers and clients. In versions 4.1.124.Final, and 4.2.0.Alpha3 through 4.2.4.Final, Netty incorrectly accepts standalone newline characters (LF) as a chunk-size line terminator, regardless of a preceding carriage return (CR), instead of requiring CRLF per HTTP/1.1 standards. When combined with reverse proxies that parse LF differently (treating it as part of the chunk extension), attackers can craft requests that the proxy sees as one request but Netty processes as two, enabling request smuggling attacks. This is fixed in versions 4.1.125.Final and 4.2.5.Final.		0.0004	0.11986
CVE-2025-55163	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.124.Final and 4.2.4.Final, Netty is vulnerable to MadeYouReset DDoS. This is a logical vulnerability in the HTTP/2 protocol, that uses malformed HTTP/2 control frames in order to break the max concurrent streams limit - which results in resource exhaustion and distributed denial of service. This issue has been patched in versions 4.1.124.Final and 4.2.4.Final.		0.00036	0.10605
CVE-2025-8916	Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. BC Java bcpkix on All (API modules), Legion of the Bouncy Castle Inc. BC Java bcprov on All (API modules), Legion of the Bouncy Castle Inc. BCPKIX FIPS bcpkix-fips on All (API modules) allows Excessive Allocation. This vulnerability is associated with program files https://github.Com/bcgit/bc-java/blob/main/pkix/src/main/java/org/bouncycastle/pkix/jcajce/PKIXCertPathReviewer.Java, https://github.Com/bcgit/bc-java/blob/main/prov/src/main/java/org/bouncycastle/x509/PKIXCertPathReviewer.Java. This issue affects BC Java: from 1.44 through 1.78; BC Java: from 1.44 through 1.78; BCPKIX FIPS: from 1.0.0 through 1.0.7, from 2.0.0 through 2.0.7.		0.00036	0.10607
CVE-2026-33809	A maliciously crafted TIFF file can cause image decoding to attempt to allocate up 4GiB of memory, causing either excessive resource consumption or an out-of-memory error.		0.00036	0.10459
CVE-2025-65637	A denial-of-service vulnerability exists in github.com/sirupsen/logrus when using Entry.Writer() to log a single-line payload larger than 64KB without newline characters. Due to limitations in the internal bufio.Scanner, the read fails with "token too long" and the writer pipe is closed, leaving Writer() unusable and causing application unavailability (DoS). This affects versions < 1.8.3, 1.9.0, and 1.9.2. The issue is fixed in 1.8.3, 1.9.1, and 1.9.3+, where the input is chunked and the writer continues to function even if an error is logged.		0.00035	0.10038
CVE-2025-68161	The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25.2 does not perform TLS hostname verification of the peer certificate, even when the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName configuration attribute or the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property is set to true. This issue may allow a man-in-the-middle attacker to intercept or redirect log traffic under the following conditions: * The attacker is able to intercept or redirect network traffic between the client and the log receiver. * The attacker can present a server certificate issued by a certification authority trusted by the Socket Appender’s configured trust store (or by the default Java trust store if no custom trust store is configured). Users are advised to upgrade to Apache Log4j Core version 2.25.3, which addresses this issue. As an alternative mitigation, the Socket Appender may be configured to use a private or restricted trust root to limit the set of trusted certificates.		0.00034	0.09775
CVE-2020-29652	A nil pointer dereference in the golang.org/x/crypto/ssh component through v0.0.0-20201203163018-be400aefbc4c for Go allows remote attackers to cause a denial of service against SSH servers.		0.00031	0.08674
CVE-2026-33870	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, Netty incorrectly parses quoted strings in HTTP/1.1 chunked transfer encoding extension values, enabling request smuggling attacks. Versions 4.1.132.Final and 4.2.10.Final fix the issue.		0.0003	0.0864
CVE-2025-67735	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.129.Final and 4.2.8.Final, the		0.00028	0.07658

	`io.netty.handler.codec.http.HttpRequestEncoder` has a CRLF injection with the request URI when constructing a request. This leads to request smuggling when `HttpRequestEncoder` is used without proper sanitization of the URI. Any application / framework using `HttpRequestEncoder` can be subject to be abused to perform request smuggling using CRLF injection. Versions 4.1.129.Final and 4.2.8.Final fix the issue.			
CVE-2023-44981	Authorization Bypass Through User-Controlled Key vulnerability in Apache ZooKeeper. If SASL Quorum Peer authentication is enabled in ZooKeeper (quorum.auth.enableSasl=true), the authorization is done by verifying that the instance part in SASL authentication ID is listed in zoo.cfg server list. The instance part in SASL auth ID is optional and if it's missing, like 'eve@EXAMPLE.COM', the authorization check will be skipped. As a result an arbitrary endpoint could join the cluster and begin propagating counterfeit changes to the leader, essentially giving it complete read-write access to the data tree. Quorum Peer authentication is not enabled by default. Users are recommended to upgrade to version 3.9.1, 3.8.3, 3.7.2, which fixes the issue. Alternately ensure the ensemble election/quorum communication is protected by a firewall as this will mitigate the issue. See the documentation for more details on correct cluster administration.		0.00027	0.07262
CVE-2025-11966	In Eclipse Vert.x versions [4.0.0, 4.5.21] and [5.0.0, 5.0.4], when "directory listing" is enabled, file and directory names are inserted into generated HTML without proper escaping in the href, title, and link attributes. An attacker who can create or rename files or directories within a served path can craft filenames containing malicious script or HTML content, leading to stored cross-site scripting (XSS) that executes in the context of users viewing the affected directory listing.		0.00027	0.0732
CVE-2025-22870	Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.		0.00026	0.06984
CVE-2026-24281	Hostname verification in Apache ZooKeeper ZKTrustManager falls back to reverse DNS (PTR) when IP SAN validation fails, allowing attackers who control or spoof PTR records to impersonate ZooKeeper servers or clients with a valid certificate for the PTR name. It's important to note that attacker must present a certificate which is trusted by ZKTrustManager which makes the attack vector harder to exploit. Users are recommended to upgrade to version 3.8.6 or 3.9.5, which fixes this issue by introducing a new configuration option to disable reverse DNS lookup in client and quorum protocols.		0.00026	0.06952
CVE-2025-48924	Uncontrolled Recursion vulnerability in Apache Commons Lang. This issue affects Apache Commons Lang: Starting with commons-lang:commons-lang 2.0 to 2.6, and, from org.apache.commons:commons-lang3 3.0 before 3.18.0. The methods ClassUtils.getClass(...) can throw StackOverflowError on very long inputs. Because an Error is usually not handled by applications and libraries, a StackOverflowError could cause an application to stop. Users are recommended to upgrade to version 3.18.0, which fixes the issue.		0.00025	0.06729
CVE-2026-21452	MessagePack for Java is a serializer implementation for Java. A denial-of-service vulnerability exists in versions prior to 0.9.11 when deserializing .msgpack files containing EXT32 objects with attacker-controlled payload lengths. While MessagePack-Java parses extension headers lazily, it later trusts the declared EXT payload length when materializing the extension data. When ExtensionValue.getData() is invoked, the library attempts to allocate a byte array of the declared length without enforcing any upper bound. A malicious .msgpack file of only a few bytes can therefore trigger unbounded heap allocation, resulting in JVM heap exhaustion, process termination, or service unavailability. This vulnerability is triggered during model loading / deserialization, making it a model format vulnerability suitable for remote exploitation. The vulnerability enables a remote denial-of-service attack against applications that deserialize untrusted .msgpack model files using MessagePack for Java. A specially crafted but syntactically valid .msgpack file containing an EXT32 object with an attacker-controlled, excessively large payload length can trigger unbounded memory allocation during deserialization. When the model file is loaded, the library trusts the declared length metadata and attempts to allocate a byte array of that size, leading to rapid heap exhaustion, excessive garbage collection, or immediate JVM termination with an OutOfMemoryError. The attack requires no malformed bytes, user interaction, or elevated privileges and can be exploited remotely in real-world environments such as model registries, inference services, CI/CD pipelines, and cloud-based model hosting platforms that accept		0.00023	0.06044

	or fetch .msgpack artifacts. Because the malicious file is extremely small yet valid, it can bypass basic validation and scanning mechanisms, resulting in complete service unavailability and potential cascading failures in production systems. Version 0.9.11 fixes the vulnerability.			
CVE-2025-47914	SSH Agent servers do not validate the size of messages when processing new identity requests, which may cause the program to panic if the message is malformed due to an out of bounds read.		0.00021	0.05584
CVE-2026-1002	The Vert.x Web static handler component cache can be manipulated to deny the access to static files served by the handler using specifically crafted request URI. The issue comes from an improper implementation of the C. rule of section 5.2.4 of RFC3986 and is fixed in Vert.x Core component (used by Vert.x Web): https://github.com/eclipse-vertx/vert.x/pull/5895 Steps to reproduce Given a file served by the static handler, craft an URI that introduces a string like bar%2F..%2F after the last / char to deny the access to the URI with an HTTP 404 response. For example https://example.com/foo/index.html can be denied with https://example.com/foo/bar%2F..%2Findex.html Mitgation Disabling Static Handler cache fixes the issue. StaticHandler staticHandler = StaticHandler.create().setCachingEnabled(false);		0.00021	0.05611
CVE-2026-24308	Improper handling of configuration values in ZKConfig in Apache ZooKeeper 3.8.5 and 3.9.4 on all platforms allows an attacker to expose sensitive information stored in client configuration in the client's logfile. Configuration values are exposed at INFO level logging rendering potential production systems affected by the issue. Users are recommended to upgrade to version 3.8.6 or 3.9.5 which fixes this issue.		0.00021	0.05441
CVE-2024-23944	Information disclosure in persistent watchers handling in Apache ZooKeeper due to missing ACL check. It allows an attacker to monitor child znodes by attaching a persistent watcher (addWatch command) to a parent which the attacker has already access to. ZooKeeper server doesn't do ACL check when the persistent watcher is triggered and as a consequence, the full path of znodes that a watch event gets triggered upon is exposed to the owner of the watcher. It's important to note that only the path is exposed by this vulnerability, not the data of znode, but since znode path can contain sensitive information like user name or login ID, this issue is potentially critical. Users are recommended to upgrade to version 3.9.2, 3.8.4 which fixes the issue.		0.00019	0.04856
CVE-2024-29371	In jose4j before 0.9.6, an attacker can cause a Denial-of-Service (DoS) condition by crafting a malicious JSON Web Encryption (JWE) token with an exceptionally high compression ratio. When this token is processed by the server, it results in significant memory allocation and processing time during decompression.		0.00019	0.05068
CVE-2022-41727	An attacker can craft a malformed TIFF image which will consume a significant amount of memory when passed to DecodeConfig. This could lead to a denial of service.		0.00018	0.0432
CVE-2024-25710	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to version 1.26.0 which fixes the issue.		0.00018	0.0457
CVE-2021-43565	The x/crypto/ssh package before 0.0.0-20211202192323-5770296d904e of golang.org/x/crypto allows an attacker to panic an SSH server.		0.00015	0.03161
CVE-2026-33186	gRPC-Go is the Go language implementation of gRPC. Versions prior to 1.79.3 have an authorization bypass resulting from improper input validation of the HTTP/2 `:path` pseudo-header. The gRPC-Go server was too lenient in its routing logic, accepting requests where the `:path` omitted the mandatory leading slash (e.g., `Service/Method` instead of `/Service/Method`). While the server successfully routed these requests to the correct handler, authorization interceptors (including the official `grpc/authz` package) evaluated the raw, non-canonical path string. Consequently, "deny" rules defined using canonical paths (starting with `/`) failed to match the incoming request, allowing it to bypass the policy if a fallback "allow" rule was present. This affects gRPC-Go servers that use path-based authorization interceptors, such as the official RBAC implementation in `google.golang.org/grpc/authz` or custom interceptors relying on `info.FullMethod` or `grpc.Method(ctx)`; AND that have a security policy contains specific "deny" rules for canonical paths but allows other requests by default (a fallback "allow" rule). The vulnerability is		0.00014	0.02497

	exploitable by an attacker who can send raw HTTP/2 frames with malformed `:path` headers directly to the gRPC server. The fix in version 1.79.3 ensures that any request with a `:path` that does not start with a leading slash is immediately rejected with a `codes.Unimplemented` error, preventing it from reaching authorization interceptors or handlers with a non-canonical path string. While upgrading is the most secure and recommended path, users can mitigate the vulnerability using one of the following methods: Use a validating interceptor (recommended mitigation); infrastructure-level normalization; and/or policy hardening.			
CVE-2026-1225	ACE vulnerability in configuration file processing by QOS.CH logback-core up to and including version 1.5.24 in Java applications, allows an attacker to instantiate classes already present on the class path by compromising an existing logback configuration file. The instantiation of a potentially malicious Java class requires that said class is present on the user's class-path. In addition, the attacker must have write access to a configuration file. However, after successful instantiation, the instance is very likely to be discarded with no further ado.		0.00012	0.01653
CVE-2026-24400	AssertJ provides Fluent testing assertions for Java and the Java Virtual Machine (JVM). Starting in version 1.4.0 and prior to version 3.27.7, an XML External Entity (XXE) vulnerability exists in `org.assertj.core.util.xml.XmlStringPrettyFormatter`: the `toXmlDocument(String)` method initializes `DocumentBuilderFactory` with default settings, without disabling DTDs or external entities. This formatter is used by the `isXmlEqualTo(CharSequence)` assertion for `CharSequence` values. An application is vulnerable only when it uses untrusted XML input with either `isXmlEqualTo(CharSequence)` from `org.assertj.core.api.AbstractCharSequenceAssert` or `xmlPrettyFormat(String)` from `org.assertj.core.util.xml.XmlStringPrettyFormatter`. If untrusted XML input is processed by tone of these methods, an attacker couldnread arbitrary local files via `file://` URIs (e.g., `/etc/passwd`, application configuration files); perform Server-Side Request Forgery (SSRF) via HTTP/HTTPS URIs, and/or cause Denial of Service via "Billion Laughs" entity expansion attacks. `isXmlEqualTo(CharSequence)` has been deprecated in favor of XMLUnit in version 3.18.0 and will be removed in version 4.0. Users of affected versions should, in order of preference: replace `isXmlEqualTo(CharSequence)` with XMLUnit, upgrade to version 3.27.7, or avoid using `isXmlEqualTo(CharSequence)` or `XmlStringPrettyFormatter` with untrusted input. `XmlStringPrettyFormatter` has historically been considered a utility for `isXmlEqualTo(CharSequence)` rather than a feature for AssertJ users, so it is deprecated in version 3.27.7 and removed in version 4.0, with no replacement.		0.00012	0.01707
GHSA-58qw-p7qm-5rvh	### From the reporter > `XmlParser` is vulnerable to XML external entity (XXE) vulnerability. > XmlParser is being used when parsing Jetty’s xml configuration files. An attacker might exploit > this vulnerability in order to achieve SSRF or cause a denial of service. > One possible scenario is importing a (remote) malicious WAR into a Jetty’s server, while the > WAR includes a malicious web.xml. ### Impact There are no circumstances in a normally deployed Jetty server where potentially hostile XML is given to the XmlParser class without the attacker already having arbitrary access to the server. I.e. in order to exploit `XmlParser` the attacker would already have the ability to deploy and execute hostile code. Specifically, Jetty has no protection against malicious web application and potentially hostile web applications should only be run on an isolated virtualisation. Thus this is not considered a vulnerability of the Jetty server itself, as any such usage of the jetty XmlParser is equally vulnerable as a direct usage of the JVM supplied SAX parser. No CVE will be allocated to this advisory. However, any direct usage of the `XmlParser` class by an application may be vulnerable. The impact would greatly depend on how the application uses `XmlParser`, but it could be a denial of service due to large entity expansion, or possibly the revealing local files if the XML results are accessible remotely. ### Patches Ability to configure the SAXParserFactory to fit the needs of your particular XML parser implementation have been merged as part of PR #10067 ### Workarounds Don't use Jetty's `XmlParser` to parse data from users.		None	None
GHSA-6g3j-p5g6-992f	### Impact A flaw was discovered in OpenSearch, affecting the `_search` API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service. The issue was identified by Elastic Engineering and corresponds to security advisory [ESA-2023-14](https://discuss.elastic.co/t/elasticsearch-8-9-1-7-17-13-security-update/343297) (CVE-2023-31419). ### Mitigation Versions 1.3.14 and 2.11.1 contain a fix for this issue. ### For more information If you have any questions or comments about this advisory, please contact AWS/Amazon Security via our issue reporting page (https://		None	None

	aws.amazon.com/security/vulnerability-reporting/) or directly via email to aws-security@amazon.com. Please do not create a public GitHub issue.			
GHSA-72hv-8253-57qq	### Summary The non-blocking (async) JSON parser in `jackson-core` bypasses the `maxNumberLength` constraint (default: 1000 characters) defined in `StreamReadConstraints`. This allows an attacker to send JSON with arbitrarily long numbers through the async parser API, leading to excessive memory allocation and potential CPU exhaustion, resulting in a Denial of Service (DoS). The standard synchronous parser correctly enforces this limit, but the async parser fails to do so, creating an inconsistent enforcement policy. ### Details The root cause is that the async parsing path in `NonBlockingUtf8JsonParserBase` (and related classes) does not call the methods responsible for number length validation. - The number parsing methods (e.g., `_finishNumberIntegralPart`) accumulate digits into the `TextBuffer` without any length checks. - After parsing, they call `_valueComplete()`, which finalizes the token but does **not** call `resetInt()` or `resetFloat()`. - The `resetInt()`/`resetFloat()` methods in `ParserBase` are where the `validateIntegerLength()` and `validateFPLength()` checks are performed. - Because this validation step is skipped, the `maxNumberLength` constraint is never enforced in the async code path. ### PoC The following JUnit 5 test demonstrates the vulnerability. It shows that the async parser accepts a 5,000-digit number, whereas the limit should be 1,000. ```java package tools.jackson.core.unittest.dos; import java.nio.charset.StandardCharsets; import org.junit.jupiter.api.Test; import tools.jackson.core.*; import tools.jackson.core.exc.StreamConstraintsException; import tools.jackson.core.json.JsonFactory; import tools.jackson.core.json.async.NonBlockingByteArrayJsonParser; import static org.junit.jupiter.api.Assertions.*; /** * POC: Number Length Constraint Bypass in Non-Blocking (Async) JSON Parsers * * Authors: sprabhav7, rohan-repos * * maxNumberLength default = 1000 characters (digits). * A number with more than 1000 digits should be rejected by any parser. * * BUG: The async parser never calls resetInt()/ resetFloat() which is where * validateIntegerLength()/validateFPLength() lives. Instead it calls * _valueComplete() which skips all number length validation. * * CWE-770: Allocation of Resources Without Limits or Throttling */ class AsyncParserNumberLengthBypassTest { private static final int MAX_NUMBER_LENGTH = 1000; private static final int TEST_NUMBER_LENGTH = 5000; private final JsonFactory factory = new JsonFactory(); // CONTROL: Sync parser correctly rejects a number exceeding maxNumberLength @Test void syncParserRejectsLongNumber() throws Exception { byte[] payload = buildPayloadWithLongInteger(TEST_NUMBER_LENGTH); // Output to console System.out.println("[SYNC] Parsing " + TEST_NUMBER_LENGTH + "-digit number (limit: " + MAX_NUMBER_LENGTH + ")"); try { try (JsonParser p = factory.createParser(ObjectReadContext.empty(), payload)) { while (p.nextToken() != null) { if (p.currentToken() == JsonToken.VALUE_NUMBER_INT) { System.out.println("[SYNC] Accepted number with " + p.getText().length() + " digits — UNEXPECTED"); } } } fail("Sync parser must reject a " + TEST_NUMBER_LENGTH + "-digit number"); } catch (StreamConstraintsException e) { System.out.println("[SYNC] Rejected with StreamConstraintsException: " + e.getMessage()); } } // VULNERABILITY: Async parser accepts the SAME number that sync rejects @Test void asyncParserAcceptsLongNumber() throws Exception { byte[] payload = buildPayloadWithLongInteger(TEST_NUMBER_LENGTH); NonBlockingByteArrayJsonParser p = (NonBlockingByteArrayJsonParser) factory.createNonBlockingByteArrayParser(ObjectReadContext.empty()); p.feedInput(payload, 0, payload.length); p.endOfInput(); boolean foundNumber = false; try { while (p.nextToken() != null) { if (p.currentToken() == JsonToken.VALUE_NUMBER_INT) { foundNumber = true; String numberText = p.getText(); assertEquals(TEST_NUMBER_LENGTH, numberText.length(), "Async parser silently accepted all " + TEST_NUMBER_LENGTH + " digits"); } } // Output to console System.out.println("[ASYNC INT] Accepted number with " + TEST_NUMBER_LENGTH + " digits — BUG CONFIRMED"); assertTrue(foundNumber, "Parser should have produced a VALUE_NUMBER_INT token"); } catch (StreamConstraintsException e) { fail("Bug is fixed — async parser now correctly rejects long numbers: " + e.getMessage()); } p.close(); } private byte[] buildPayloadWithLongInteger(int numDigits) { StringBuilder sb = new StringBuilder(numDigits + 10); sb.append("{\"v\":"); for (int i = 0; i < numDigits; i++) { sb.append((char) ('1' + (i % 9))); } sb.append('}'); return sb.toString().getBytes(StandardCharsets.UTF_8); } } ``` ### Impact A malicious actor can send a JSON document with an arbitrarily long number to an application using the async parser (e.g., in a Spring WebFlux or other reactive application). This can cause: 1. **Memory Exhaustion:** Unbounded allocation of memory in the `TextBuffer` to store the number's digits, leading to an `OutOfMemoryError`. 2. **CPU		None	None

	Exhaustion:** If the application subsequently calls `getBigIntegerValue()` or `getDecimalValue()`, the JVM can be tied up in O(n^2) `BigInteger` parsing operations, leading to a CPU-based DoS. ### Suggested Remediation The async parsing path should be updated to respect the `maxNumberLength` constraint. The simplest fix appears to ensure that `_valueComplete()` or a similar method in the async path calls the appropriate validation methods (`resetInt()` or `resetFloat()`) already present in `ParserBase`, mirroring the behavior of the synchronous parsers. **NOTE:** This research was performed in collaboration with [rohan-repos](https://github.com/rohan-repos)			
GHSA-m425-mq94-257g	### Impact In affected releases of gRPC-Go, it is possible for an attacker to send HTTP/2 requests, cancel them, and send subsequent requests, which is valid by the HTTP/2 protocol, but would cause the gRPC-Go server to launch more concurrent method handlers than the configured maximum stream limit. ### Patches This vulnerability was addressed by #6703 and has been included in patch releases: 1.56.3, 1.57.1, 1.58.3. It is also included in the latest release, 1.59.0. Along with applying the patch, users should also ensure they are using the `grpc.MaxConcurrentStreams` server option to apply a limit to the server's resources used for any single connection. ### Workarounds None. ### References #6703		None	None
GHSA-xpw8-rcwv-8f8p	A client might overload the server by issue frequent RST frames. This can cause a massive amount of load on the remote system and so cause a DDOS attack. ### Impact This is a DDOS attack, any http2 server is affected and so you should update as soon as possible. ### Patches This is patched in version 4.1.100.Final. ### Workarounds A user can limit the amount of RST frames that are accepted per connection over a timeframe manually using either an own `Http2FrameListener` implementation or an `ChannelInboundHandler` implementation (depending which http2 API is used). ### References - https://www.cve.org/CVERecord?id=CVE-2023-44487 - https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ - https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/		None	None