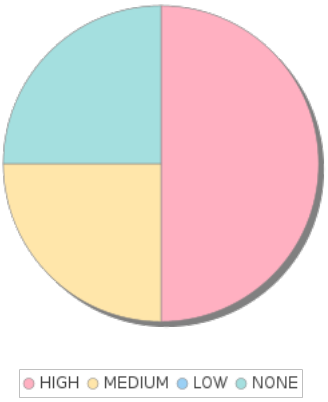
ASSESSMENT REPORT

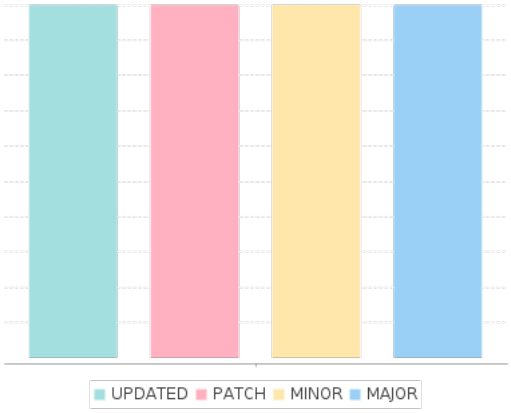
Project: **nanaorg/java-ex**
Branch: **meterian-bot/pr/be7e3526-69fe-4a65-8cc6-c3cbdf9e82bd**
(72edf26e9784167f246a69bef58e48967245d26a)

Created on **2023-10-03 16:28 UTC**

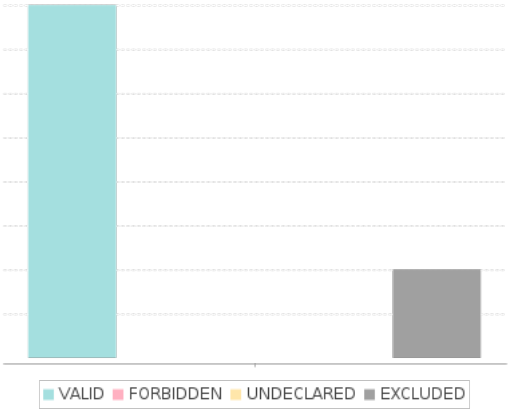
Security - 0



Stability - 99



Licensing - 100



Security Assessment:
We have identified potential security issues in the libraries this project is using. You can find all the details in the security assessments below. While your code might not expose you to the security threat at the moment, it's recommended to go through each of them and update your libraries to a non-vulnerable version.
Score: 0

Stability Assessment:
There are new patch releases available for one or more of the project dependencies declared in this project. You will find all the details in the stability section below. It is recommended to update your dependencies to the latest patch release to benefit of all the latest bugfixes. While you are looking at it, consider also having a look at the new minor and major releases (in the same table) that can offer you more advanced features.
Score: 99

Licensing Assessment:
Our analysis shows that at the moment this project code does not violate any of the licensing policies that were provided.
Score: 100

SECURITY ASSESSMENT

Library (java)

ch.qos.logback:logback-core - 1.1.11 (compile) — Severity: CRITICAL

Description:

QOS.ch Logback before 1.2.0 has a serialization vulnerability affecting the SocketServer and ServerSocketReceiver components.

More Info:

- https://logback.qos.ch/news.html
- https://nvd.nist.gov/vuln/detail/CVE-2017-5929
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    ch.qos.logback:logback-core:1.1.11

ch.qos.logback:logback-core - 1.1.11 (compile) — Severity: MEDIUM

Description:

In logback version 1.2.9 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.

More Info:

- CVE-2021-42550
- https://github.com/cn-panda/logbackRceDemo
- https://jira.qos.ch/browse/LOGBACK-1591
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    ch.qos.logback:logback-core:1.1.11

com.google.protobuf:protobuf-java - 3.6.1 (compile) **Severity:** HIGH

Description:

A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2022-3171
- CVE-2022-3171
- https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16
        com.google.protobuf:protobuf-java:3.6.1

com.google.protobuf:protobuf-java - 3.6.1 (compile) **Severity:** HIGH

Description:

A parsing issue similar to CVE-2022-3171, but with textformat in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2022-3509
- https://github.com/protocolbuffers/protobuf/commit/a3888f53317a8018e7a439bac4abeb8f3425d5e9
- https://github.com/advisories/GHSA-g5ww-5jh7-63cx
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16
        com.google.protobuf:protobuf-java:3.6.1

com.google.protobuf:protobuf-java - 3.6.1 (compile) **Severity: HIGH**

Description:

A parsing issue similar to CVE-2022-3171, but with Message-Type Extensions in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2022-3510
- https://github.com/protocolbuffers/protobuf/commit/db7c17803320525722f45c1d26fc08bc41d1bf48
- https://github.com/advisories/GHSA-4gg5-vx3j-xwc7
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16
        com.google.protobuf:protobuf-java:3.6.1

com.google.protobuf:protobuf-java - 3.6.1 (compile) **Severity: MEDIUM**

Description:

Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

More Info:

- CVE-2021-22570
- https://github.com/protocolbuffers/protobuf/releases/tag/v3.15.0
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/IFX6KPNOFHYD6L4XES5PCM3QNSKZBOTQ/
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16
        com.google.protobuf:protobuf-java:3.6.1

com.google.protobuf:protobuf-java - 3.6.1 (compile) **Severity: MEDIUM**

Description:

An issue in protobuf-java allowed the interleaving of com.google.protobuf.UnknownFieldSet fields in such a way that would be processed out of order. A small malicious payload can occupy the parser for several minutes by creating large numbers of short-lived objects that cause frequent, repeated pauses. We recommend upgrading libraries beyond the vulnerable versions.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-22569
- CVE-2021-22569
- https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=39330
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16
        com.google.protobuf:protobuf-java:3.6.1

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: CRITICAL**

Description:

In order to decrypt SM2 encrypted data an application is expected to call the API function EVP*PKEY*decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP*PKEY*decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP*PKEY*decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP*PKEY*decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-3711
- CVE-2021-3711
- https://www.openssl.org/news/secadv/20210824.txt
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity:** HIGH

Description:

Due to the formatting logic of the "console.table()" function it was not safe to allow user controlled input to be passed to the "properties" parameter while simultaneously passing a plain object with at least one property as the first parameter, which could be "proto". The prototype pollution has very limited control, in that it only allows an empty string to be assigned to numerical keys of the object prototype.Node.js >= 12.22.9, >= 14.18.3, >= 16.13.2, and >= 17.3.1 use a null protoype for the object these properties are being assigned to.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2022-21824
- CVE-2022-21824
- https://hackerone.com/reports/1431042
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity:** HIGH

Description:

Server or client applications that call the SSL*check*chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature*algorithms*cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-1967
- CVE-2020-1967
- https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=eb563247aef3e83dda7679c43f9649270462e5b1
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: HIGH**

Description:

ASN.1 strings are represented internally within OpenSSL as an ASN1*STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1*STRING*set() function will additionally NUL terminate the byte array in the ASN1*STRING structure. However, it is possible for applications to directly construct valid ASN1*STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1*STRING array. This can also happen by using the ASN1*STRING*set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1*STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1*STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1*STRING structures). It can also occur in the X509*get1*email(), X509*REQ*get1*email() and X509*get1*ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1*STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).*

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-3712
- CVE-2021-3712
- https://www.openssl.org/news/secadv/20210824.txt
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: HIGH**

Description:

The X509*V*FLAG*X509*STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named "purpose" values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509*V*FLAG*X509*STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-3450
- CVE-2021-3450
- https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2a40b7bc7b94dd7de897a74571e7024f0cf0d63b
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: HIGH**

Description:

Accepting arbitrary Subject Alternative Name (SAN) types, unless a PKI is specifically defined to use a particular SAN type, can result in bypassing name-constrained intermediates. Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 was accepting URI SAN types, which PKIs are often not defined to use. Additionally, when a protocol allows URI SANs, Node.js did not match the URI correctly.Versions of Node.js with the fix for this disable the URI SAN type when checking a certificate against a hostname. This behavior can be reverted through the --security-revert command-line option.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-44531
- CVE-2021-44531
- https://hackerone.com/reports/1429694
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2022-21363
- https://www.oracle.com/security-alerts/cpujan2022.html
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:H).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-2471
- CVE-2021-2471
- https://www.oracle.com/security-alerts/cpuoct2021.html
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature*algorithms extension (where it was present in the initial ClientHello), but includes a signature*algorithms *cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).*

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-3449
- CVE-2021-3449
- https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fb9fa6b51defd48157eeb207f52181f735d96148
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 converts SANs (Subject Alternative Names) to a string format. It uses this string to check peer certificates against hostnames when validating connections. The string format was subject to an injection vulnerability when name constraints were used within a certificate chain, allowing the bypass of these name constraints.Versions of Node.js with the fix for this escape SANs containing the problematic characters in order to prevent the injection. This behavior can be reverted through the --security-revert command-line option.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-44532
- CVE-2021-44532
- https://hackerone.com/reports/1429694
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 did not handle multi-value Relative Distinguished Names correctly. Attackers could craft certificate subjects containing a single-value Relative Distinguished Name that would be interpreted as a multi-value Relative Distinguished Name, for example, in order to inject a Common Name that would allow bypassing the certificate subject verification.Affected versions of Node.js that do not accept multi-value Relative Distinguished Names and are thus not vulnerable to such attacks themselves. However, third-party code that uses node's ambiguous presentation of certificate subjects may be vulnerable.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-44533
- CVE-2021-44533
- https://hackerone.com/reports/1429694
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors as well as unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2023-21971
- CVE-2023-21971
- https://www.oracle.com/security-alerts/cpuapr2023.html
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

mysql:mysql-connector-java - 8.0.16 (compile) **Severity: MEDIUM**

Description:

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.19 and prior and 5.1.48 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. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-2934
- CVE-2020-2934
- https://www.oracle.com/security-alerts/cpuapr2020.html
- (registry)

Locations:

/pom.xml

Hierarchy:

com.meterian.qa.samples:java-sample-failing:1.0
    mysql:mysql-connector-java:8.0.16

STABILITY ASSESSMENT

Library (java)	New patch	New minor	New major
ch.qos.logback:logback-core 1.1.11 (compile) (registry)	1.1.11	1.4.11	-
junit:junit 3.8.2 (compile) (registry)	3.8.2	-	4.13.2
mysql:mysql-connector-java 8.0.16 (compile) (registry)	8.0.33	-	-

LICENSING ASSESSMENT

Libraries (java)

ch.qos.logback:logback-core 1.1.11 (compile)
EPL-1.0
LGPL-2.1
LGPL-2.0-only
(registry)

com.google.protobuf:protobuf-java 3.6.1 (compile) (transitive)
BSD-3-Clause
(registry)

com.meterian.qa.samples:java-sample-failing 1.0 (root)
BSD
unapplicable - Excluded by account whitelisting
(registry)

junit:junit 3.8.2 (compile)
CPL-1.0
(registry)

mysql:mysql-connector-java 8.0.16 (compile)
GPL-2.0-only
(registry)

REPORTED EXCLUSIONS

You can find listed here all the applicable exclusions you reported in regards to the advice contained in this report.