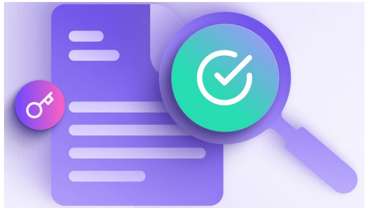
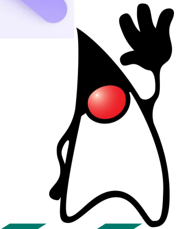
Trust in Software Supply Chain





Reproducible Builds

Maven

maven central

Hervé Boutemy

2025-04-25

CHAINS https://chains.proj.kth.se

About Me: Hervé Boutemy

- Java, since 1.0-beta
- framework based on OSS
- CI, DevOps
- Enterprise Architecture
- DevSecOps

sonatype

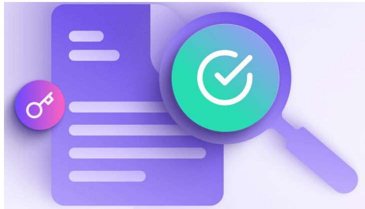
- Solutions Architect
- Software Supply Chain

About Me: *Hervé Boutemy*

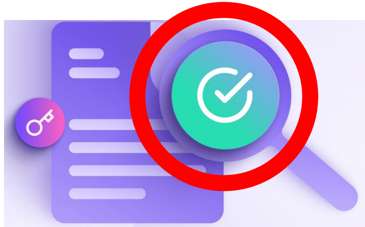
- Apache Maven PMC Chair
- Apache Software Foundation Member

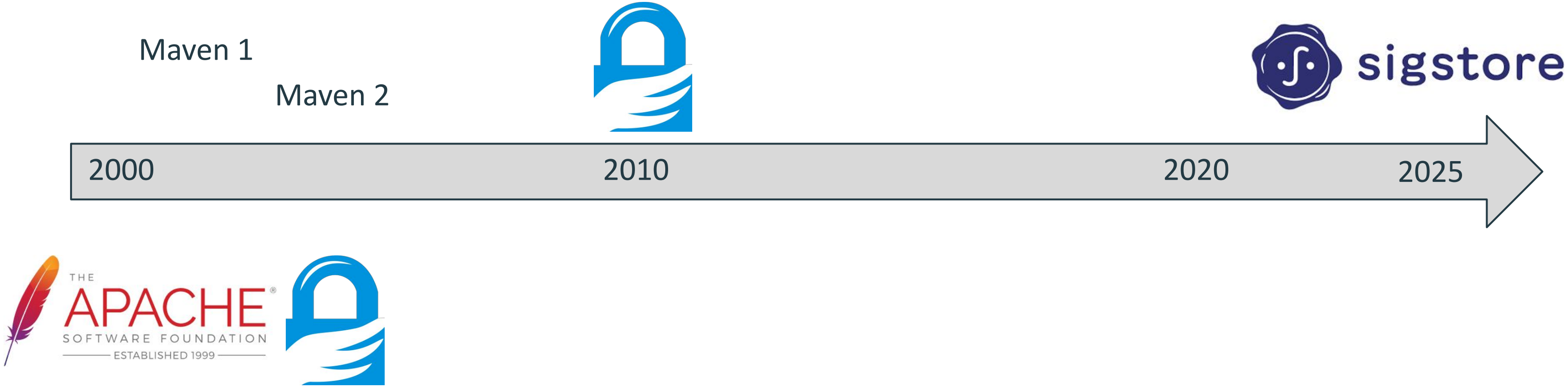
- SBOM: CycloneDX, SPDX
- signature: Sigstore

- Reproducible Builds for the JVM:
  - discovered in April 2016 (post-processing)
  - actively working since January 2019 (Maven built-in)



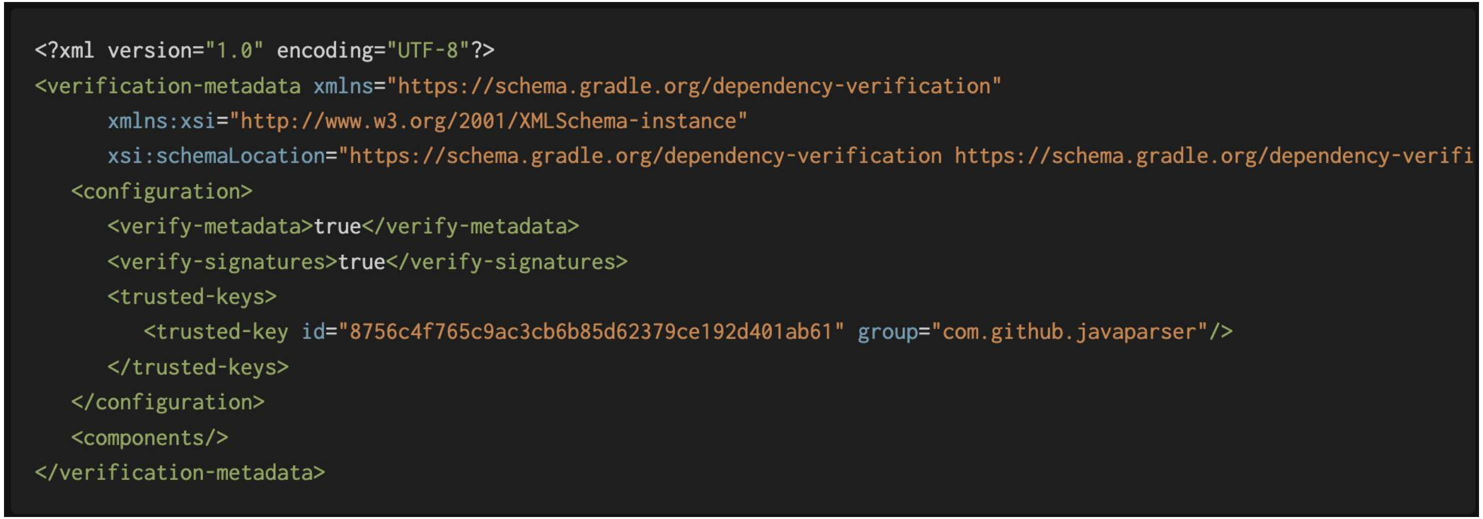
maven central &





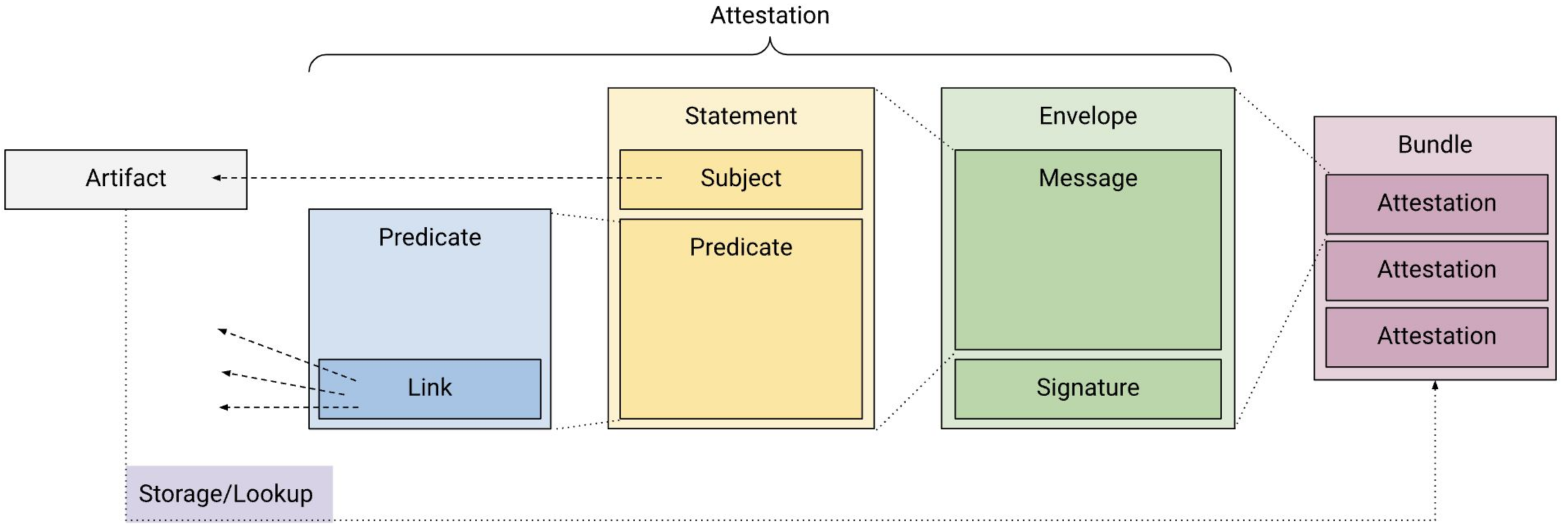
Gradle

Verifying dependencies



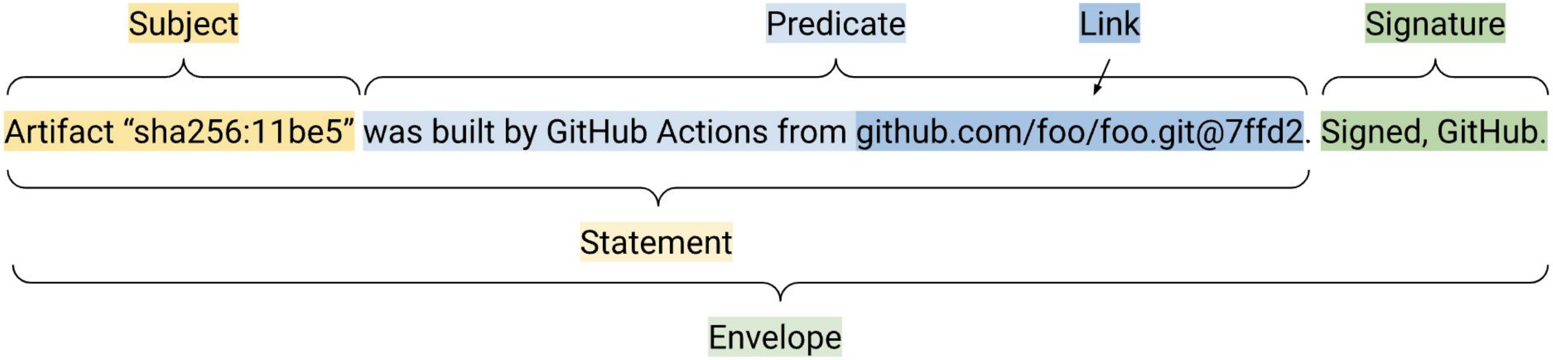
```
<?xml version="1.0" encoding="UTF-8"?>
<verification-metadata xmlns="https://schema.gradle.org/dependency-verification"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="https://schema.gradle.org/dependency-verification https://schema.gradle.org/dependency-verifi
   <configuration>
      <verify-metadata>true</verify-metadata>
      <verify-signatures>true</verify-signatures>
      <trusted-keys>
         <trusted-key id="8756c4f765c9ac3cb6b85d62379ce192d401ab61" group="com.github.javaparser"/>
      </trusted-keys>
   </configuration>
   <components/>
</verification-metadata>
```

SLSA



Attestation
Statement
Envelope
Bundle
Artifact
Subject
Message
Attestation
Predicate
Predicate
Attestation
Attestation
Link
Signature
Storage/Lookup

SLSA Provenance



Subject

Predicate

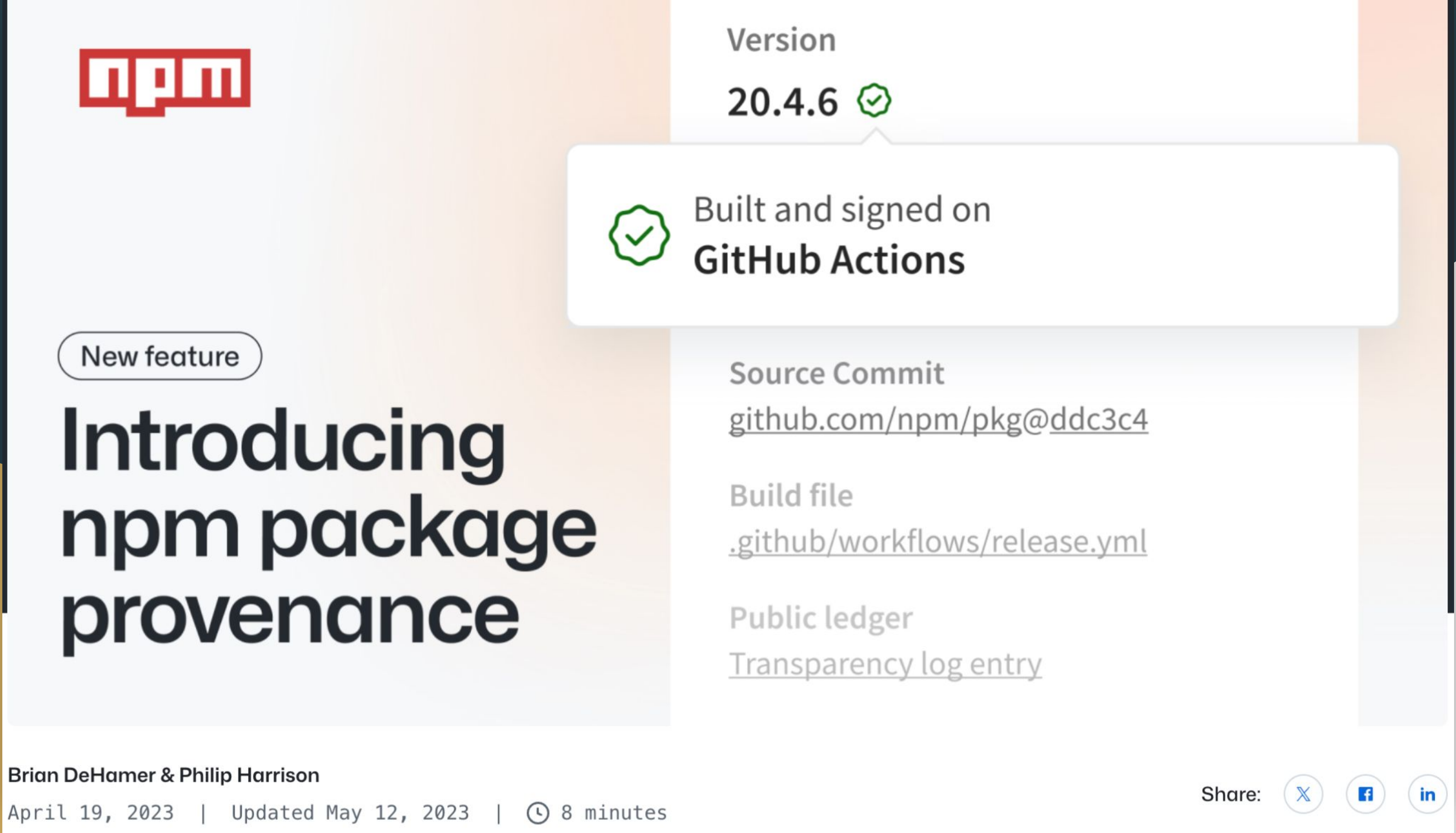
Link

Signature

Artifact “sha256:11be5” was built by GitHub Actions from github.com/foo/foo.git@7ffd2. Signed, GitHub.

Statement

Envelope



New feature

Introducing npm package provenance

Version

20.4.6 ✓

Built and signed on

GitHub Actions

Source Commit

github.com/npm/pkg@ddc3c4

Build file

.github/workflows/release.yml

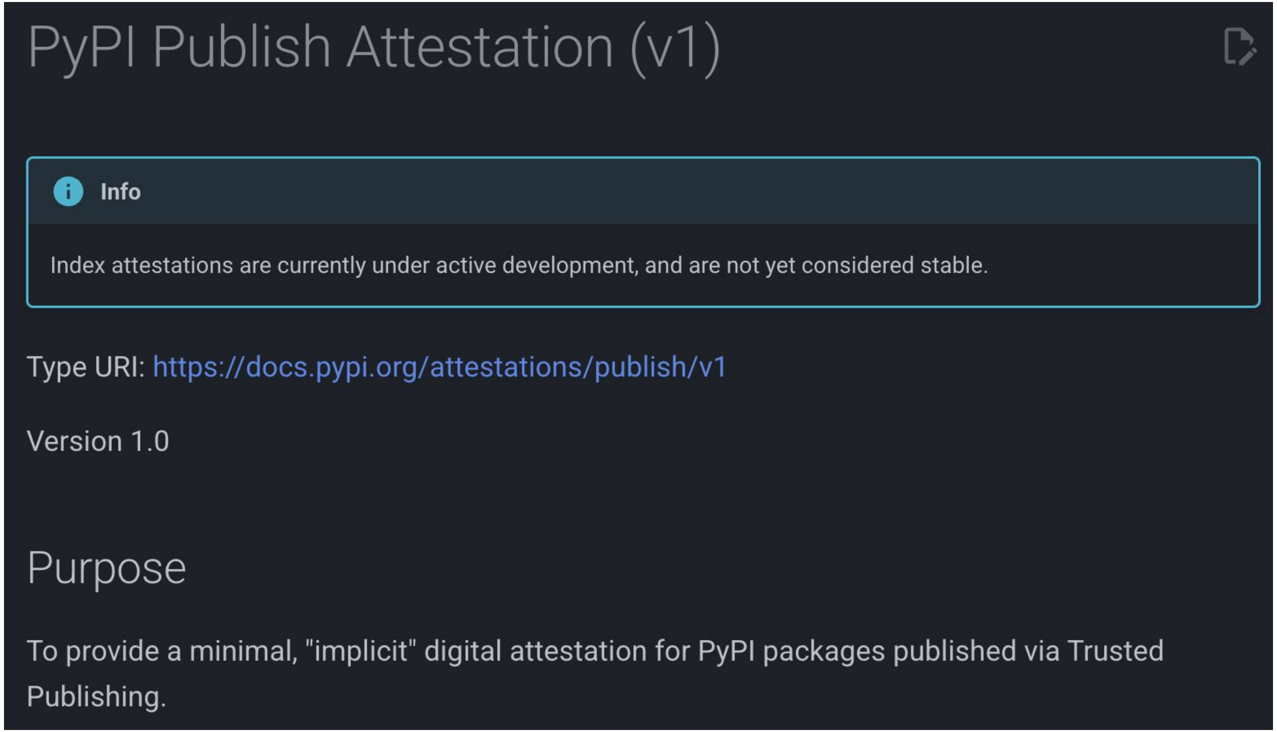
Public ledger

Transparency log entry

Brian DeHamer & Philip Harrison

April 19, 2023 | Updated May 12, 2023 | 8 minutes

Share:



PyPI Publish Attestation (v1)

Info

Index attestations are currently under active development, and are not yet considered stable.

Type URI: https://docs.pypi.org/attestations/publish/v1

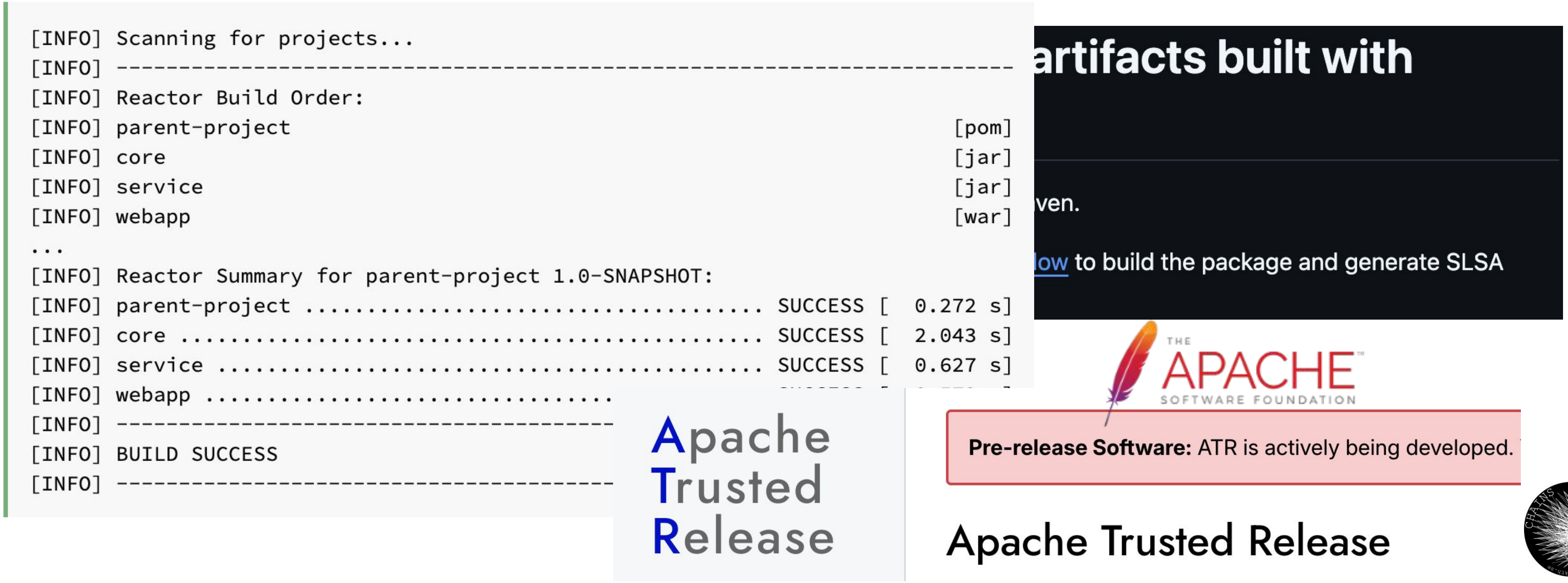
Version 1.0

Purpose

To provide a minimal, "implicit" digital attestation for PyPI packages published via Trusted Publishing.

Maven

maven central



```
[INFO] Scanning for projects...
[INFO] ------------------------------------------------------------------------
[INFO] Reactor Build Order:
[INFO] parent-project                                                     [pom]
[INFO] core                                                               [jar]
[INFO] service                                                            [jar]
[INFO] webapp                                                             [war]
...
[INFO] Reactor Summary for parent-project 1.0-SNAPSHOT:
[INFO] parent-project ..................................... SUCCESS [  0.272 s]
[INFO] core ............................................... SUCCESS [  2.043 s]
[INFO] service ............................................ SUCCESS [  0.627 s]
[INFO] webapp ................................
[INFO] ----------------------------------------
[INFO] BUILD SUCCESS
[INFO] ----------------------------------------
```

artifacts built with

ven.

low to build the package and generate SLSA

THE APACHE SOFTWARE FOUNDATION

Apache
Trusted
Release

Pre-release Software: ATR is actively being developed.

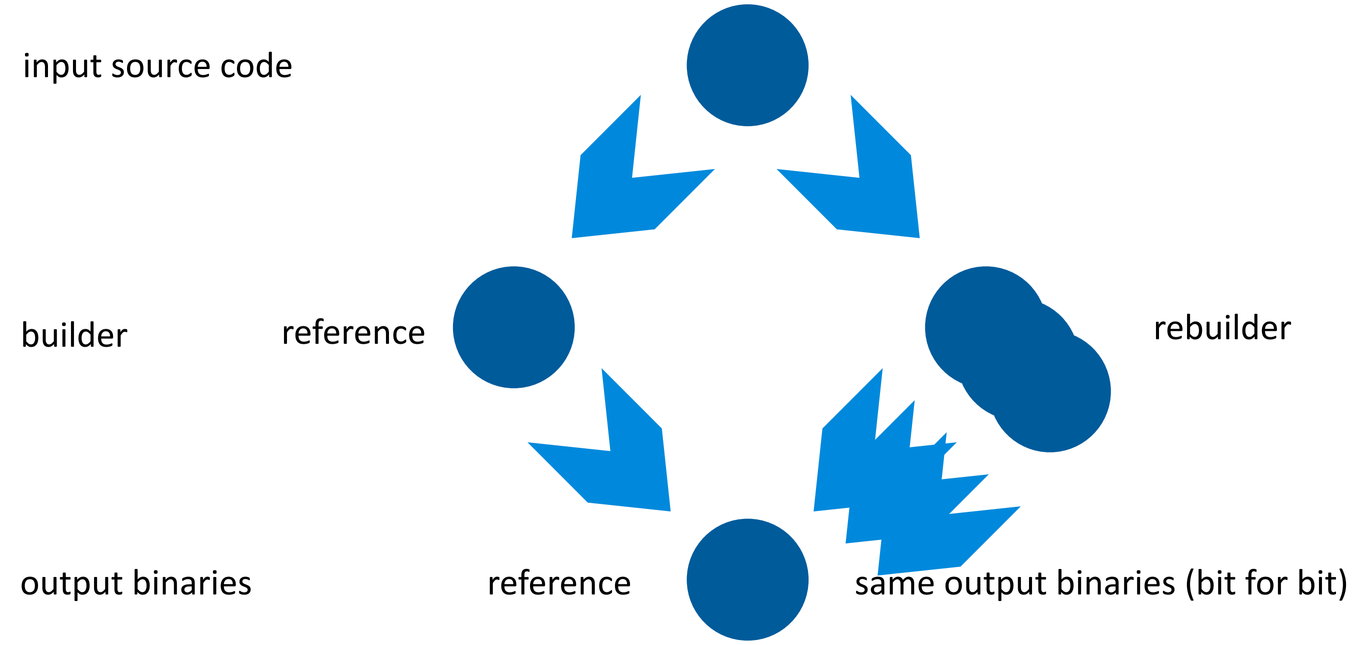
Apache Trusted Release

Reproducible Builds

Reproducible Builds

https://reproducible-builds.org/ (since 2013)

a set of software development practices that create an independently-verifiable path from source to binary code



Good News!

`javac` produces reproducible `.class` from `.java`

from the start: JDK 5, 1.4, …

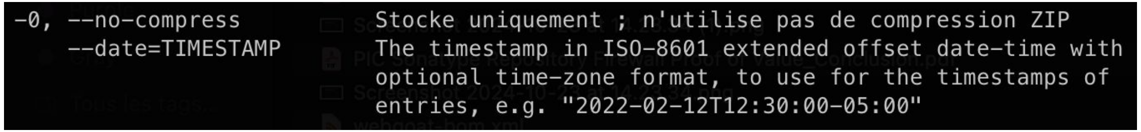
depends only on major version (not on patch, not on vendor)

few exceptions:
- 8: up to patch 345 vs after ~400
- 17: up to 17.0.13 vs 17.0.14

Bad News!

jar does not create reproducible .jar (.zip)

17



```
-0, --no-compress           Stocke uniquement ; n'utilise pas de compression ZIP
    --date=TIMESTAMP        The timestamp in ISO-8601 extended offset date-time with
                            optional time-zone format, to use for the timestamps of
                            entries, e.g. "2022-02-12T12:30:00-05:00"
```

```
<properties>
  <project.build.outputTimestamp>2023-01-01T00:00:00Z</project.build.outputTimestamp>
</properties>
```

or use Maven 4.0.0-beta-5 minimum

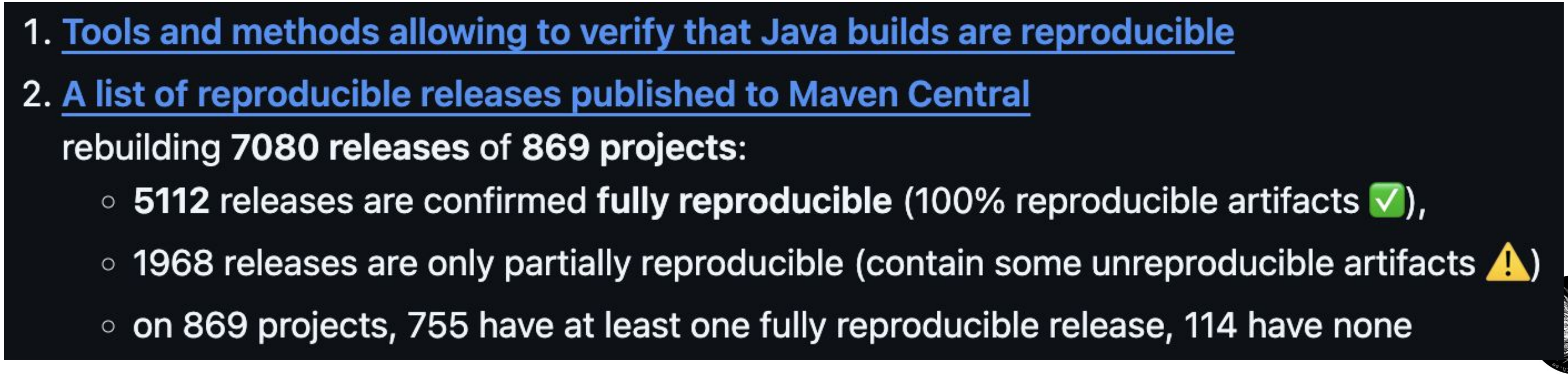
Reproducible Builds

maven central

✓ ✗

Reproducible Central (started 03-2020)

https://github.com/jvm-repo-rebuild/reproducible-central



1. Tools and methods allowing to verify that Java builds are reproducible
2. A list of reproducible releases published to Maven Central

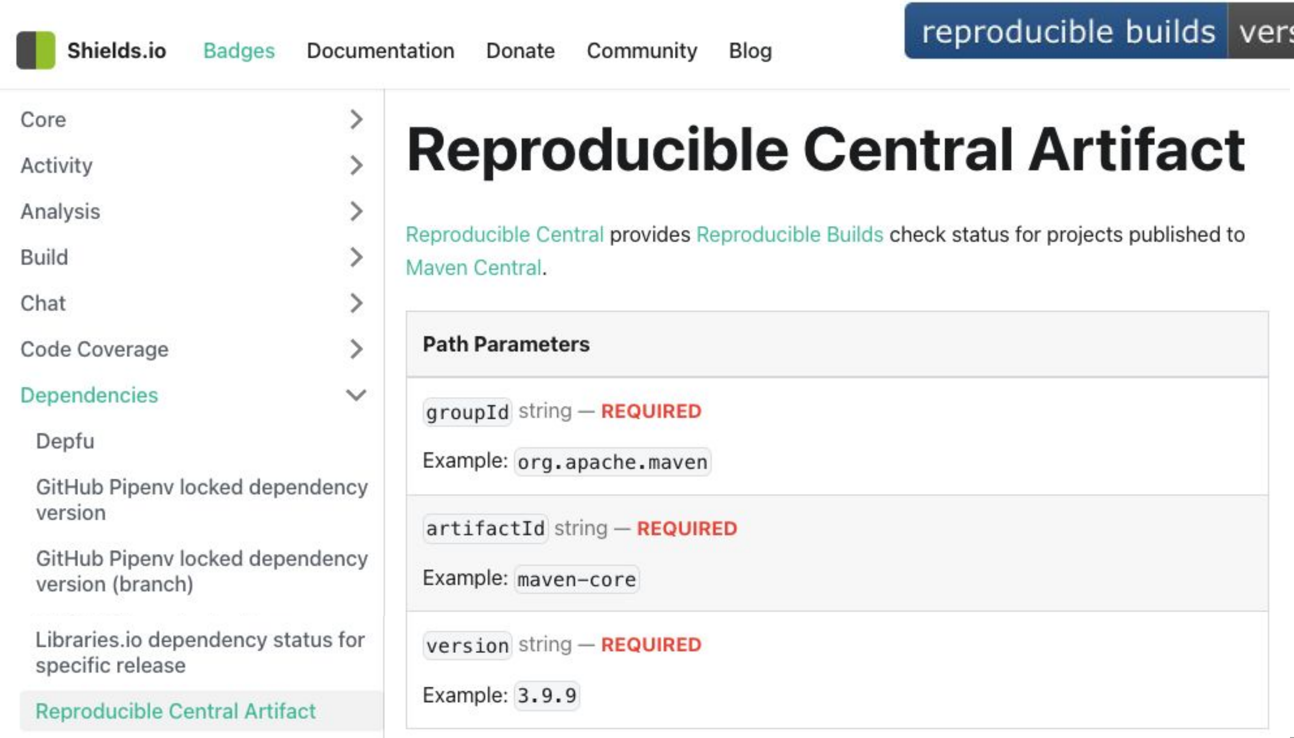
   rebuilding **7080 releases** of **869 projects**:
   - **5112** releases are confirmed **fully reproducible** (100% reproducible artifacts ✅),
   - 1968 releases are only partially reproducible (contain some unreproducible artifacts ⚠️)
   - on 869 projects, 755 have at least one fully reproducible release, 114 have none

Get Your Badge

reproducible builds 17/17

reproducible builds 3/5

reproducible builds version not evaluated



Shields.io
Badges
Documentation
Donate
Community
Blog
Core
Activity
Analysis
Build
Chat
Code Coverage
Dependencies
Depfu
GitHub Pipenv locked dependency version
GitHub Pipenv locked dependency version (branch)
Libraries.io dependency status for specific release
Reproducible Central Artifact

Reproducible Central Artifact

Reproducible Central provides Reproducible Builds check status for projects published to Maven Central.

Path Parameters

`groupId` string — **REQUIRED**

Example: `org.apache.maven`

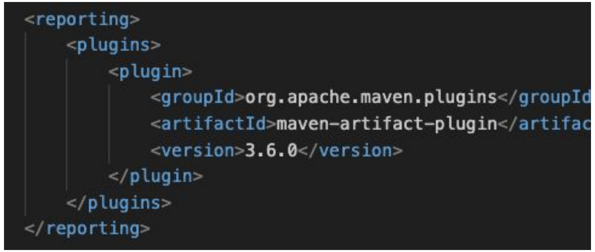
`artifactId` string — **REQUIRED**

Example: `maven-core`

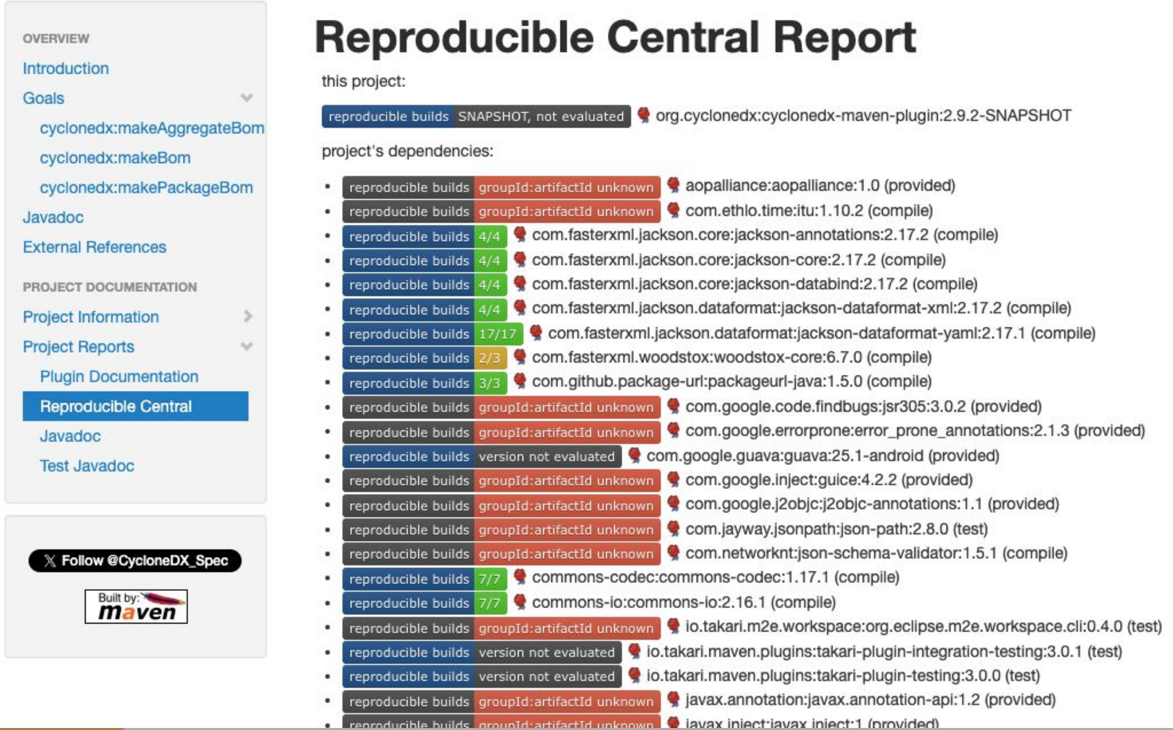
`version` string — **REQUIRED**

Example: `3.9.9`

Get a Badge for Your Dependencies



```
<reporting>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId
            <artifactId>maven-artifact-plugin</artifac
            <version>3.6.0</version>
        </plugin>
    </plugins>
</reporting>
```



Reproducible Central Report

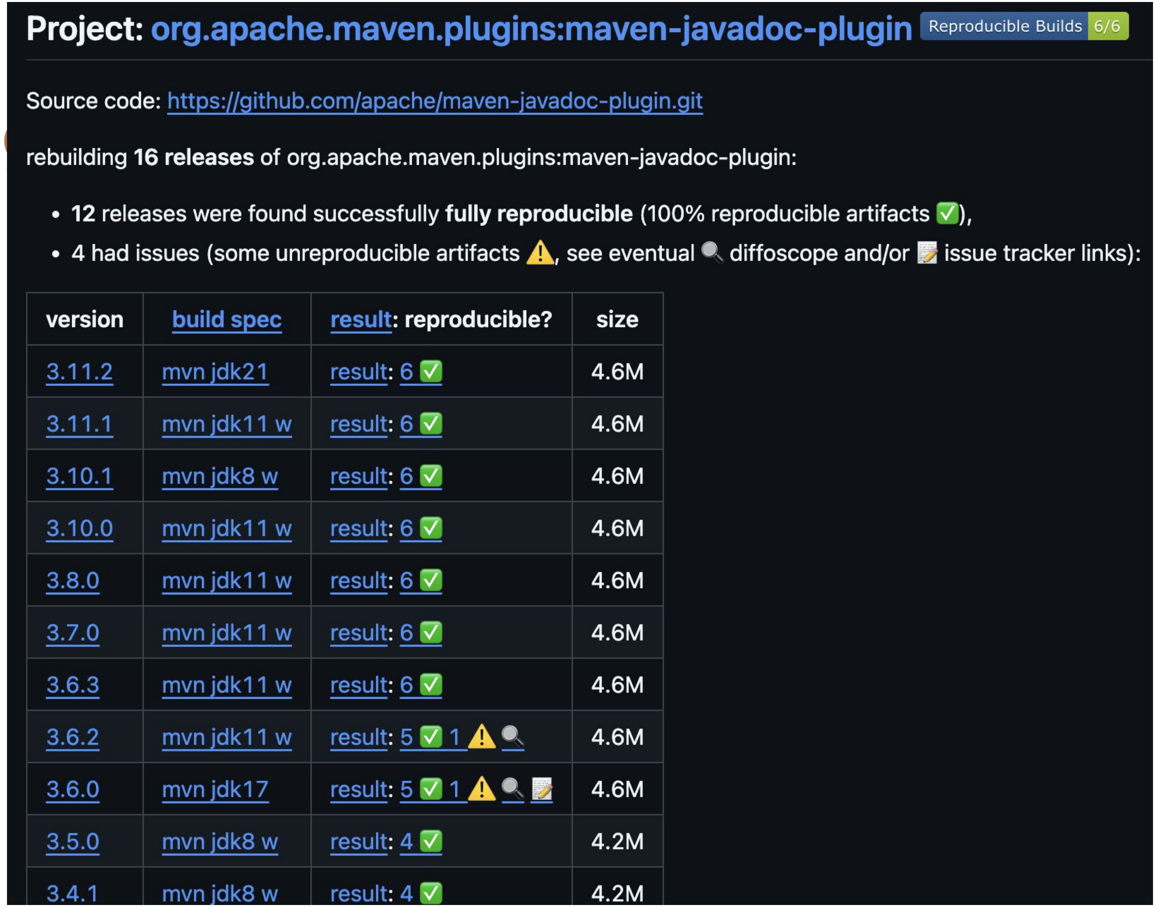
this project:

reproducible builds SNAPSHOT, not evaluated org.cyclonedx:cyclonedx-maven-plugin:2.9.2-SNAPSHOT

project's dependencies:

- reproducible builds groupId:artifactId unknown aopalliance:aopalliance:1.0 (provided)
- reproducible builds groupId:artifactId unknown com.ethlo.time:itu:1.10.2 (compile)
- reproducible builds 4/4 com.fasterxml.jackson.core:jackson-annotations:2.17.2 (compile)
- reproducible builds 4/4 com.fasterxml.jackson.core:jackson-core:2.17.2 (compile)
- reproducible builds 4/4 com.fasterxml.jackson.core:jackson-databind:2.17.2 (compile)
- reproducible builds 4/4 com.fasterxml.jackson.dataformat:jackson-dataformat-xml:2.17.2 (compile)
- reproducible builds 17/17 com.fasterxml.jackson.dataformat:jackson-dataformat-yaml:2.17.1 (compile)
- reproducible builds 2/3 com.fasterxml.woodstox:woodstox-core:6.7.0 (compile)
- reproducible builds 3/3 com.github.package-url:packageurl-java:1.5.0 (compile)
- reproducible builds groupId:artifactId unknown com.google.code.findbugs:jsr305:3.0.2 (provided)
- reproducible builds groupId:artifactId unknown com.google.errorprone:error_prone_annotations:2.1.3 (provided)
- reproducible builds version not evaluated com.google.guava:guava:25.1-android (provided)
- reproducible builds groupId:artifactId unknown com.google.inject:guice:4.2.2 (provided)
- reproducible builds groupId:artifactId unknown com.google.j2objc:j2objc-annotations:1.1 (provided)
- reproducible builds groupId:artifactId unknown com.jayway.jsonpath:json-path:2.8.0 (test)
- reproducible builds groupId:artifactId unknown com.networknt:json-schema-validator:1.5.1 (compile)
- reproducible builds 7/7 commons-codec:commons-codec:1.17.1 (compile)
- reproducible builds 7/7 commons-io:commons-io:2.16.1 (compile)
- reproducible builds groupId:artifactId unknown io.takari.m2e.workspace:org.eclipse.m2e.workspace.cli:0.4.0 (test)
- reproducible builds version not evaluated io.takari.maven.plugins:takari-plugin-integration-testing:3.0.1 (test)
- reproducible builds version not evaluated io.takari.maven.plugins:takari-plugin-testing:3.0.0 (test)
- reproducible builds groupId:artifactId unknown javax.annotation:javax.annotation-api:1.2 (provided)
- reproducible builds groupId:artifactId unknown javax.inject:javax.inject:1 (provided)

Improvin



Project: org.apache.maven.plugins:maven-javadoc-plugin

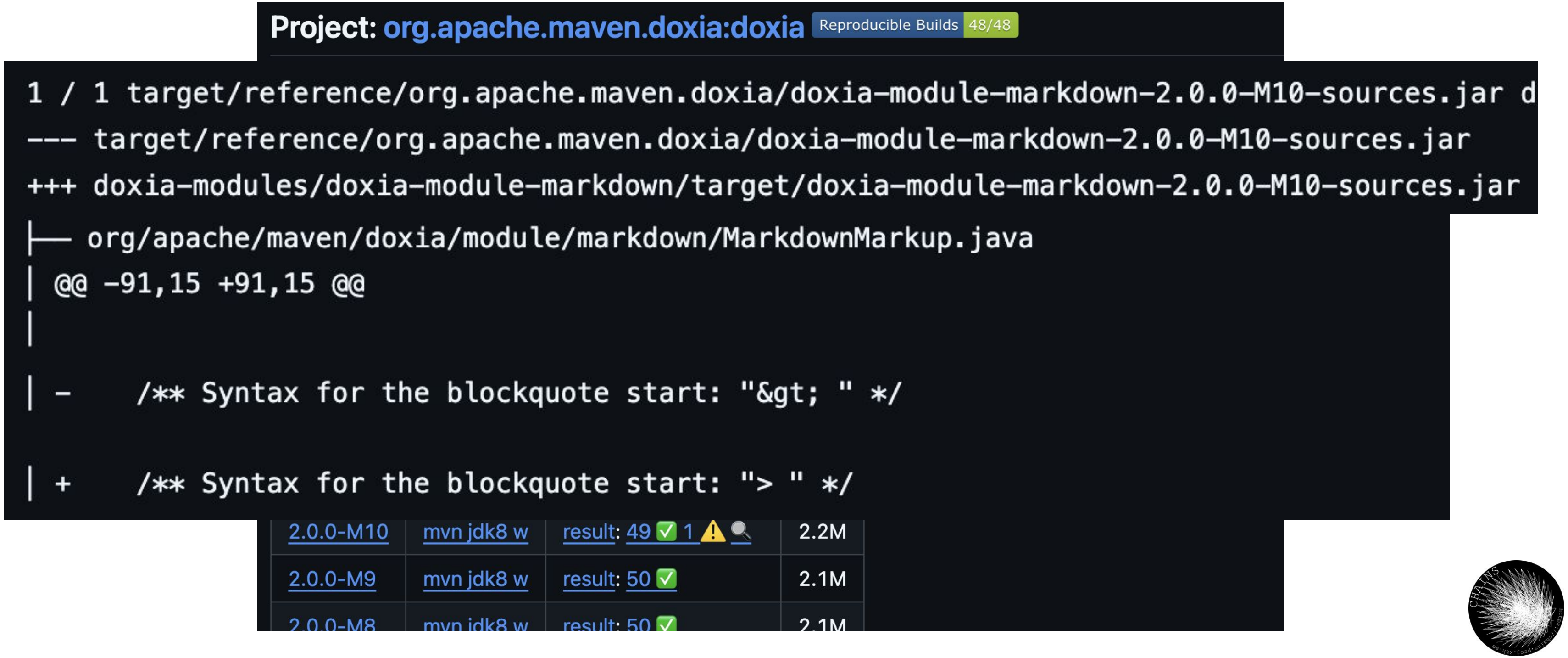
Source code: https://github.com/apache/maven-javadoc-plugin.git

rebuilding **16 releases** of org.apache.maven.plugins:maven-javadoc-plugin:

- **12** releases were found successfully **fully reproducible** (100% reproducible artifacts ✅),
- 4 had issues (some unreproducible artifacts ⚠️, see eventual 🔍 diffoscope and/or 📝 issue tracker links):

version	build spec	result: reproducible?	size
3.11.2	mvn jdk21	result: 6 ✅	4.6M
3.11.1	mvn jdk11 w	result: 6 ✅	4.6M
3.10.1	mvn jdk8 w	result: 6 ✅	4.6M
3.10.0	mvn jdk11 w	result: 6 ✅	4.6M
3.8.0	mvn jdk11 w	result: 6 ✅	4.6M
3.7.0	mvn jdk11 w	result: 6 ✅	4.6M
3.6.3	mvn jdk11 w	result: 6 ✅	4.6M
3.6.2	mvn jdk11 w	result: 5 ✅ 1 ⚠️ 🔍	4.6M
3.6.0	mvn jdk17	result: 5 ✅ 1 ⚠️ 🔍 📝	4.6M
3.5.0	mvn jdk8 w	result: 4 ✅	4.2M
3.4.1	mvn jdk8 w	result: 4 ✅	4.2M

Improving trust...



Project: org.apache.maven.doxia:doxia Reproducible Builds 48/48

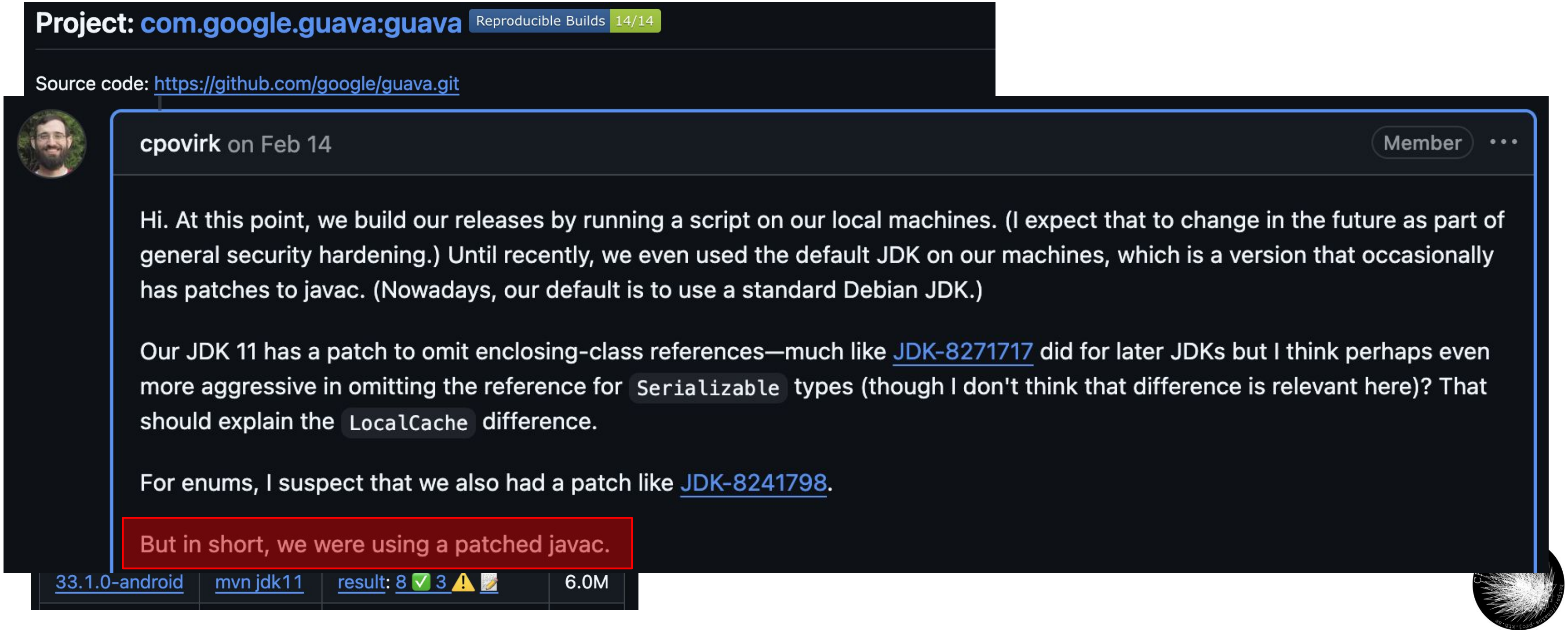
```
1 / 1 target/reference/org.apache.maven.doxia/doxia-module-markdown-2.0.0-M10-sources.jar d
--- target/reference/org.apache.maven.doxia/doxia-module-markdown-2.0.0-M10-sources.jar
+++ doxia-modules/doxia-module-markdown/target/doxia-module-markdown-2.0.0-M10-sources.jar
├── org/apache/maven/doxia/module/markdown/MarkdownMarkup.java
│ @@ -91,15 +91,15 @@
│

│ -    /** Syntax for the blockquote start: "&gt; " */

│ +    /** Syntax for the blockquote start: "> " */
```

2.0.0-M10	mvn jdk8 w	result: 49 ✅ 1 ⚠️ 🔍	2.2M
2.0.0-M9	mvn jdk8 w	result: 50 ✅	2.1M
2.0.0-M8	mvn jdk8 w	result: 50 ✅	2.1M

Improving trust...



Project: com.google.guava:guava Reproducible Builds 14/14

Source code: https://github.com/google/guava.git

cpovirk on Feb 14 Member

Hi. At this point, we build our releases by running a script on our local machines. (I expect that to change in the future as part of general security hardening.) Until recently, we even used the default JDK on our machines, which is a version that occasionally has patches to javac. (Nowadays, our default is to use a standard Debian JDK.)

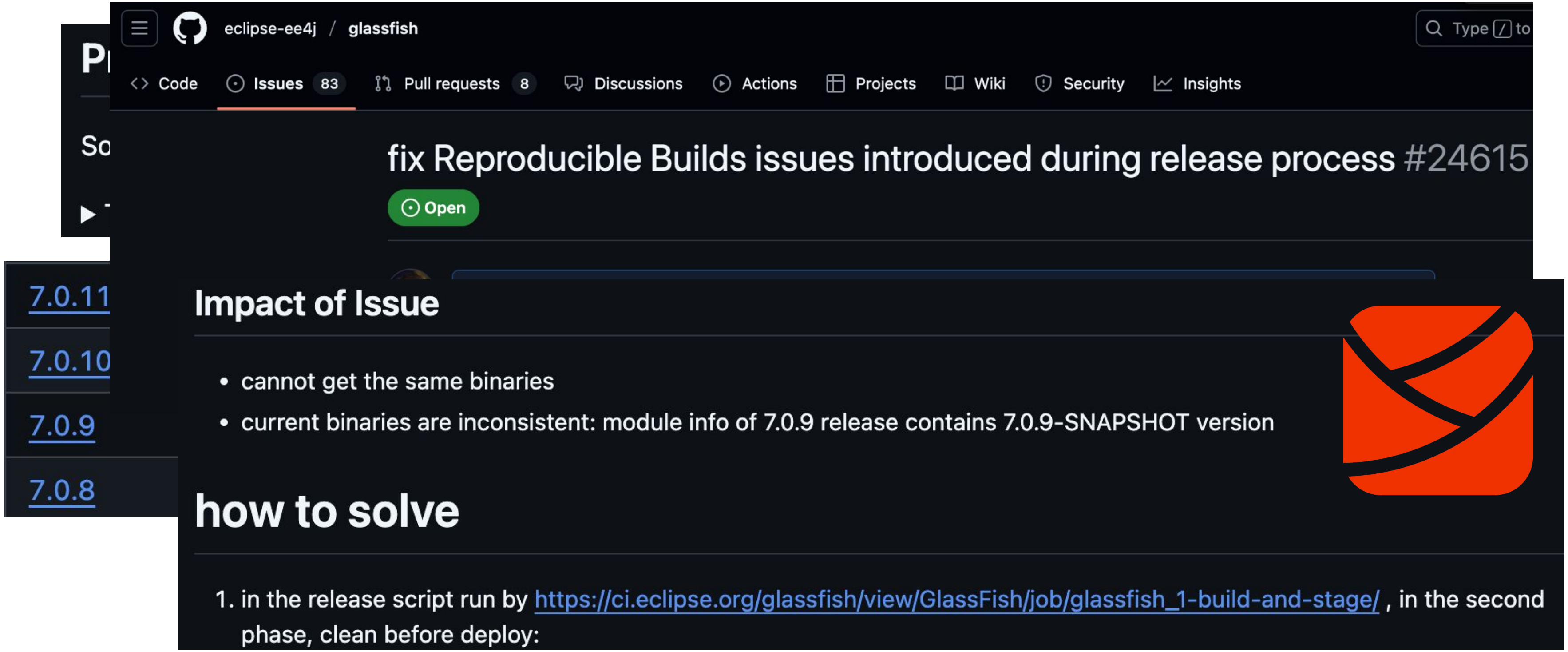
Our JDK 11 has a patch to omit enclosing-class references—much like JDK-8271717 did for later JDKs but I think perhaps even more aggressive in omitting the reference for `Serializable` types (though I don't think that difference is relevant here)? That should explain the `LocalCache` difference.

For enums, I suspect that we also had a patch like JDK-8241798.

But in short, we were using a patched javac.

33.1.0-android	mvn jdk11	result: 8 ✅ 3 ⚠️ 📝	6.0M

Improving trust...



fix Reproducible Builds issues introduced during release process #24615

Impact of Issue

- cannot get the same binaries
- current binaries are inconsistent: module info of 7.0.9 release contains 7.0.9-SNAPSHOT version

how to solve

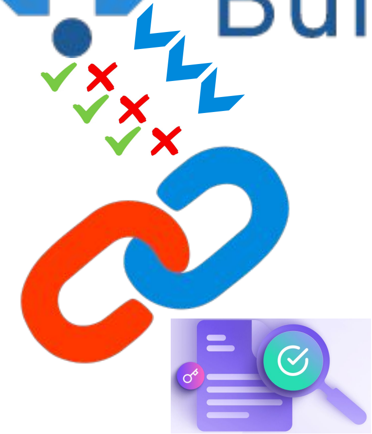
1. in the release script run by https://ci.eclipse.org/glassfish/view/GlassFish/job/glassfish_1-build-and-stage/ , in the second phase, clean before deploy:

Trust in Software Supply Chain

Creating a rebuild attestation

Reproducible Builds

maven central



Making Films Sound Better

DOLBY SYSTEM®

Noise Reduction • High Fidelity

Making Software Binaries Better

Reproducible Builds

Noise Reduction · High Confidence

Diversity in Community is Great, **not in Binary Code**

CHAINS https://chains.proj.kth.se