



/Maven-Lockfile: Locking Down the JVM Supply Chain for Hermetic Builds

Open Source Summit Europe 2026

08/10/2026



/WHO ARE WE?



PhD Student @ KTH



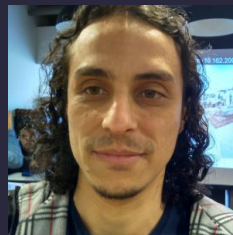
amansha@kth.se



KTH, Stockholm, Sweden



@algomaster99



Software Engineer @ Red Hat



bpimente@redhat.com



Brno, Czech Republic



@brunoapimentel



/TABLE OF CONTENTS



/01 Background

/02 Problem

/03 Hermetic Builds

/04 New Ideas





/Maven

Maven™

Java Build Tool

Declarative

```
// pom.xml
<dependency>
  <groupId>com.redhat.rcm</groupId>
  <artifactId>redhat-releng-tools</artifactId>
  <version>13</version>
</dependency>
<plugin>
  <groupId>io.github.chains-project</groupId>
  <artifactId>maven-lockfile</artifactId>
  <version>5.18.3</version>
</plugin>
```





/Why Lockfiles?



/01 Version Pinning

/02 Integrity

/03 Third Party Dependencies

/04 Hermetic Builds





/Hermetic Builds



self-contained software build process that isolates the compilation environment from the host system, relying only on explicitly declared inputs to guarantee consistent and reproducible outputs

Bazel





/Hermetic Builds



the user-defined build script:

- **MUST** declare all dependencies, including sources and other build steps, using immutable references in a format that the build service understands.

the build service:

- **MUST** fetch all artifacts in a trusted control plane.
- **MUST NOT** allow mutable references.
- **MUST** verify the integrity of each artifact.
- **MUST** prevent network access while running the build steps.





/Hermetic Builds



Why it matters?

- Reduced attack surface
- Improved reproducibility
- Accurate dependency reporting (SBOMs)
- Planned for SLSA Lv4

<https://slsa.dev/spec/v0.1/requirements#hermetic>





/Maven + Hermetic Builds?



mvn dependency:go-offline



It is not enough :(
We have evidence.



DEMO TIME





/Demo 1: Takeaway



```
[ERROR] Failed to execute goal org.apache.maven.plugins:maven-surefire-plugin:3.6.0:test (default-test) on project dynamic-resolution-capture: The following artifacts could not be resolved: org.apache.maven.surefire:surefire-junit-platform:jar:3.6.0 (absent): Cannot access central (https://repo.maven.apache.org/maven2) in offline mode and the artifact org.apache.maven.surefire:surefire-junit-platform:jar:3.6.0 has not been downloaded from it before. -> [Help 1]
```

[ERROR]

[ERROR] To see the full stack trace of the errors, re-run Maven with the **-e** switch.

[ERROR] Re-run Maven using the **-X** switch to enable full debug logging.

[ERROR]

[ERROR] For more information about the errors and possible solutions, please read the following articles:

[ERROR] **[Help 1]** <http://cwiki.apache.org/confluence/display/MAVEN/MojoExecutionException>



<https://chains.proj.kth.se/maven-hermetic-builds-blind-spot.html>





/Why?

```
// AbstractSurefireMojo.java (Surefire 3.5.6)
AbstractSurefireMojo.execute()
    → providerInfo.getProviderClasspath()
    → resolver.getProviderClasspathAsMap(..., "surefire-junit-platform",
surefireVersion)
    → repositorySystem.resolveDependencies(session, request) //
downloaded here, not declared in any POM
```

<https://github.com/apache/maven-surefire/blob/25ea054860a5c1e5932b360d8aa0a31944c2b841/maven-surefire-common/src/main/java/org/apache/maven/plugin/surefire/AbstractSurefireMojo.java#L3122-L3128>





/Maven + Hermetic Builds?



Trusted Checksums



needs Maven 3.9+





chains-project/**maven-lockfile**



Lockfiles for Maven. Pin your dependencies. Build with integrity.

 28

Contributors

 10

Used by

 65

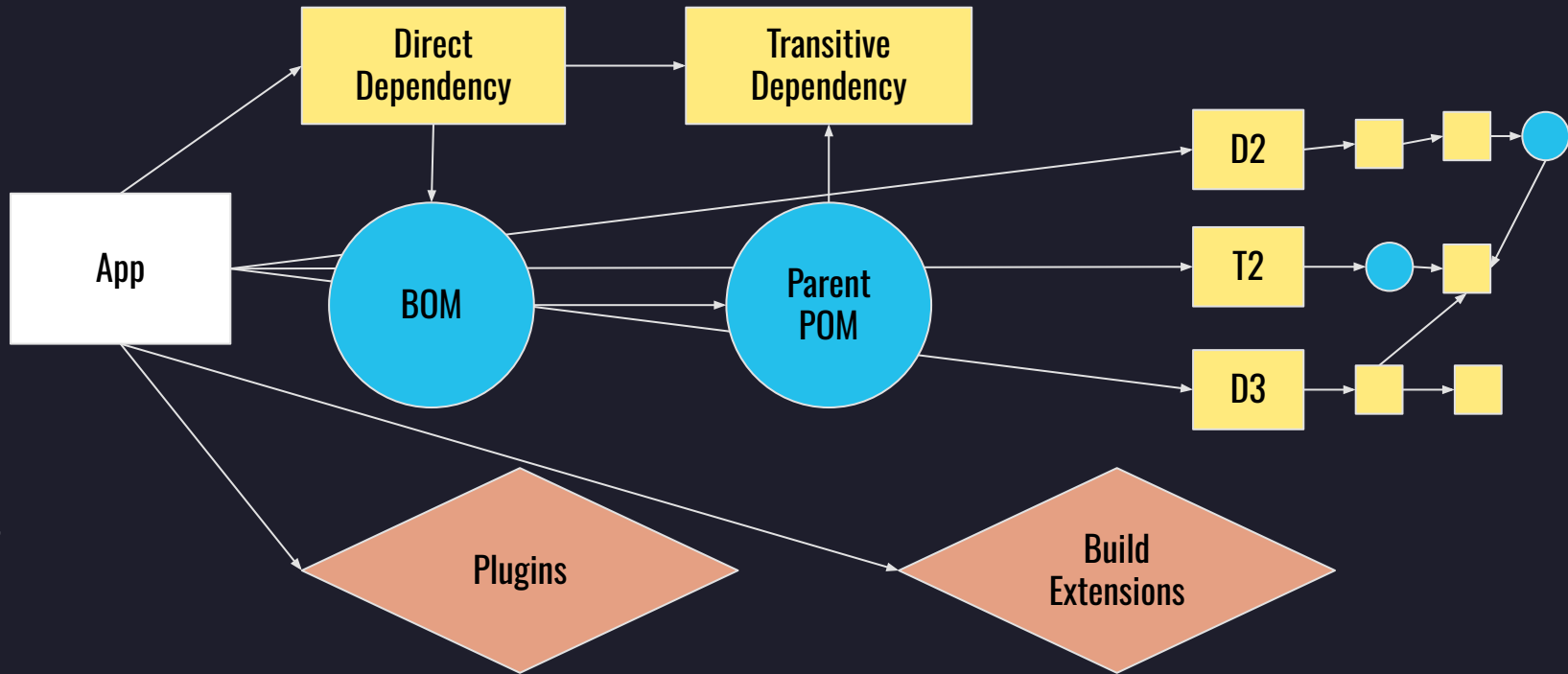
Stars

 27

Forks



```
$ mvn io.github.chains-project:maven-lockfile:generate
```





```
$ mvn io.github.chains-project:maven-lockfile:validate
```

#	Check	What's compared
1	Environment	OS, Maven version, Java version
2	Project POM	Your pom.xml: coordinates and checksum
3	Dependencies	Full dependency tree: coordinates, scope, checksum, selected version, position in the tree
4	Maven plugins	Coordinates, checksum, download URL, repository, each plugin's dependency tree
5	BOMs	Imported BOMs: coordinates, checksum, download URL, repository
6	Parent POMs	Parent POM chain of every dependency, including coordinates, checksum, repository
7	Maven extensions	Coordinates, checksum, repository, dependencies

What you build with

What you declare

Where versions come from



```
$ mvn io.github.chains-project:maven-lockfile:freeze
```

```
"dependencies": [{  
  "groupId": "com.fasterxml.jackson.core",  
  "artifactId": "jackson-databind",  
  "version": "2.22.3",  
  "checksum": "556db543...e0a9",  
  "resolved": "https://...",  
  "parentPom": {  
    "artifactId": "jackson-base",  
    "version": "2.22.3", ... },  
  "children": [  
    { "dgav" },  
    { "dgav" }]  
}]
```

```
<dependencyManagement>  
  <dgav></dgav>  
  <dgav></dgav>  
</dependencyManagement>  
<dependencies>  
  <gav>[2.22.3]</gav>  
</dependencies>  
<plugin>  
</plugin>
```



/Red Hat's Use Case

Hermetic builds are a requirement for all container-based products at Red Hat!

The hermeticity is achieved by:

- Executing each step of the build pipeline in a container
- Cutting off the network access when executing “podman build”



KONFLUX

<https://konflux-ci.dev/>

/Hermeto

A CLI tool that safely prefetches the dependencies necessary to build a project hermetically.

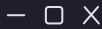
Benefits:

- simple to use
- built around supply-chain security
- produces accurate source SBOMs*

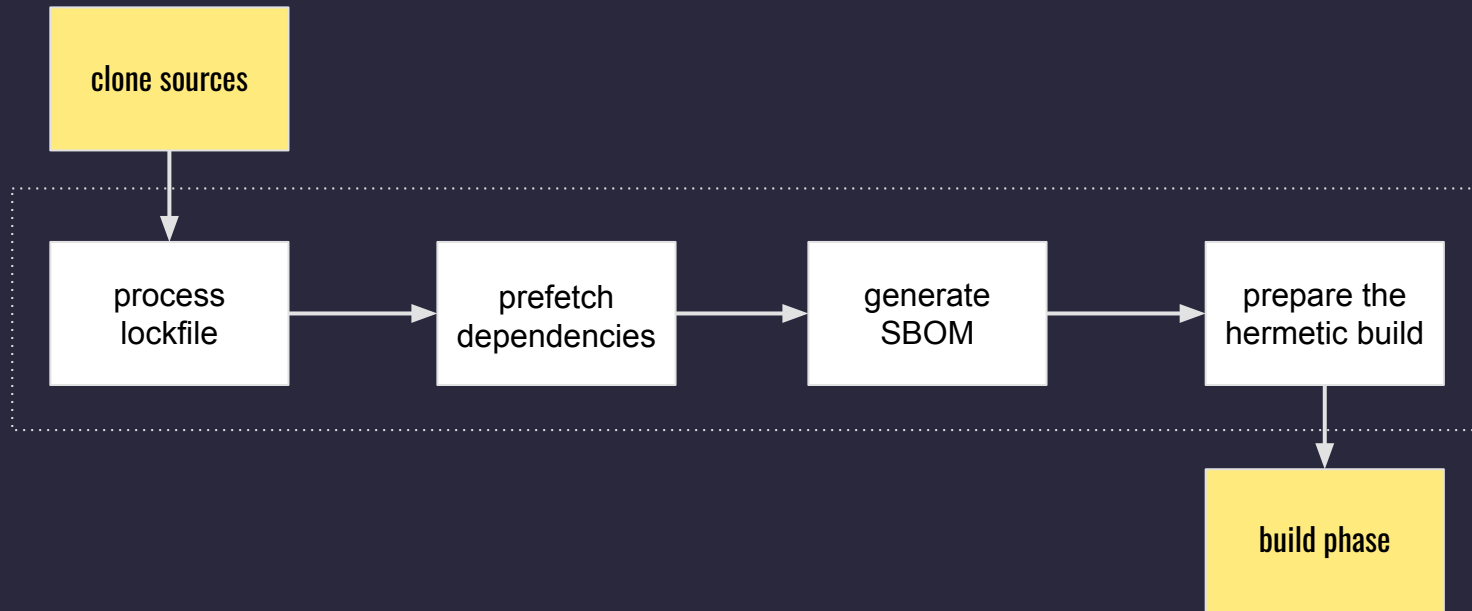


*if the build is done hermetically

<https://github.com/hermetoproject/hermeto>



/Hermeto's Workflow





/Making the Prefetch Safe

Hermeto makes the prefetch process safe by:

- preventing arbitrary code execution
- requiring explicitly defined and pinned dependencies
- verifying checksums
- applying ecosystem specific rules





/Hermeto's Supported Ecosystems



Ruby
[bundler]



Golang
[go mod]



Rust
[cargo]



Javascript
[npm, yarn, pnpm]



Python
[pip]



RPM
[dnf]





/Hermeto's Supported Ecosystems



What about Maven?





/Hermeto's Supported Ecosystems



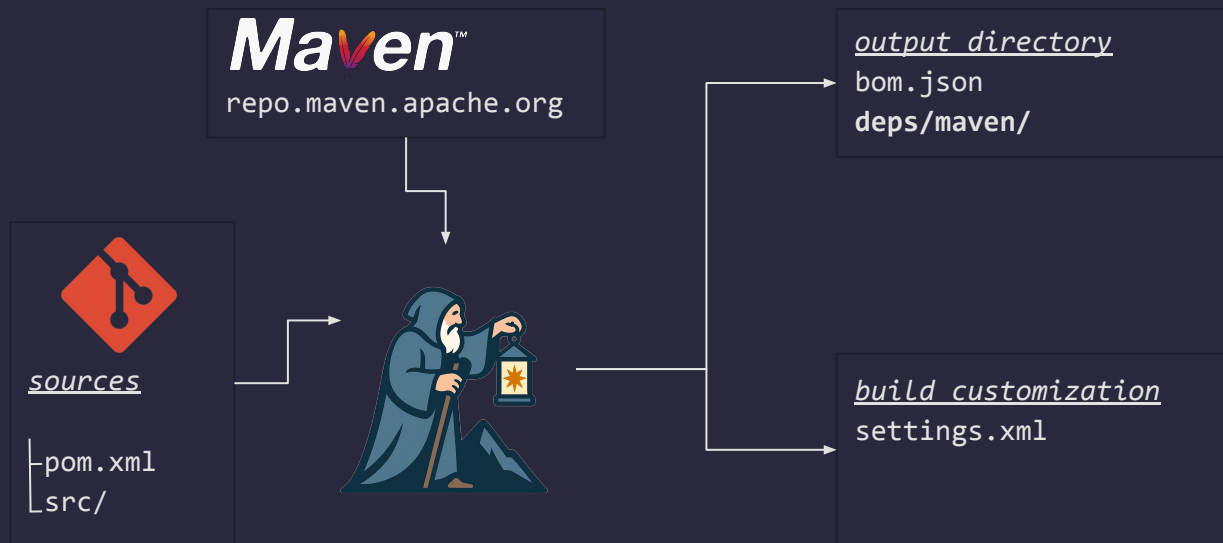
What about Maven?



Java
[maven + lockfiles]



/Hermeto + Maven Lockfile





/Hermeto + Maven Lockfile



```
$ cat Dockefile
```

```
FROM docker.io/library/maven:3.9
```

```
WORKDIR /app
```

```
COPY src src
```

```
COPY pom.xml pom.xml
```

```
RUN mvn clean package -s /tmp/hermeto/settings.xml
```

```
$ podman build \  
-t localhost/test-maven:0.1 \  
--network=none \  
-v $(realpath ./hermeto-out):/tmp/hermeto \  
.
```





/Hermeto + Maven Lockfile



```
$ hermeto fetch-deps maven \  
  --source ~/projects/js-web-app \  
  --output ./hermeto-out
```

```
$ tree ./hermeto-out
```

```
/tmp/hermeto-out  
├── bom.json  
└── deps  
    └── maven  
        └── aopalliance  
            └── 1.0  
                ├── aopalliance-1.0.jar  
                ├── aopalliance-1.0.jar.sha256  
                ├── aopalliance-1.0.pom  
                └── _remote.repositories
```

```
$ hermeto inject-files ./hermeto-out
```

```
$ cat settings.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>  
<settings ...>  
  <localRepository>/tmp/hermeto/deps/maven</localRepository>  
  <offline>true</offline>  
  <mirrors>  
    <mirror>  
      <id>hermeto-local</id>  
      <mirrorOf>*</mirrorOf>  
      <url>file:///tmp/hermeto/deps/maven</url>  
    </mirror>  
  </mirrors>  
  <profiles>  
    <profile>  
      <activation>  
        <activeByDefault>true</activeByDefault>  
      </activation>  
      <properties>  
        <maven.test.skip>true</maven.test.skip>  
      </properties>  
    </profile>  
  </profiles>  
</settings>
```





/End-to-End Demo

/Lockfile

Generate lockfile using
maven-lockfile:5.18.3

/Hermeto

```
./hermeto  
fetch-deps
```

```
./hermeto  
inject-files
```

/Run

```
mvn test
```



DEMO TIME





/GitHub Action

```
# .github/workflows/Lockfile.yml
name: Lockfile
on: pull_request

jobs:
  check-lockfile:
    runs-on: ubuntu-latest
    permissions:
      contents: write # lets the action commit an updated lockfile.json
    steps:
      - uses:
chains-project/maven-lockfile@8a6d498dd36dafd533d1dfb2fb16fce223ee0882 #
v5.18.3
        with:
          github-token: ${ secrets.GITHUB_TOKEN }
```





/Future: Automatic Dependency Update



Renovate



Dependabot

/Future: Nix Support



pchesneau on Jan 19



This would be a neat addition to maven-lockfile as it would allow, with some minor nix magic, to have a clean way to create the complete .m2 required to build any jar in nix (instead of having to manually add parent pom as nix inputs).

As of now, Since maven-lockfile is able to handle SHA-256 sum, we construct the "almost exhaustive" universe with `fetchUrl` and `linkFarm` from the lockfile, but if this feature is added, our boilerplate would totally disappear. (and it would be a very good replacement for mvn2nix)

If there is any RC version of the plugin to test, I'd be glad to make it run against our projects (some of them are quite tricky) to help with testing.



Source: <https://github.com/chains-project/maven-lockfile/issues/1439>

/Related Work

TALK **Is Maven Safe for Production?**

Adam Kaplan (Red Hat) & Manfred Moser (Chainguard)

<https://www.youtube.com/watch?v=FrcGntNgpA>

TALK **Making a Lockfile for Maven**

Adam Kaplan (Red Hat)

<https://www.youtube.com/watch?v=Wz0CWR8pV0o>

PAPER **Maven-Lockfile: High Integrity Rebuild of Past Java Releases**

Larissa Schmid, Elias Lundell, Yogya Gamage, Benoit Baudry, Martin Monperrus

<https://arxiv.org/abs/2510.00730>



/Cool Tech

CHAINS research project at KTH Royal Institute of Technology

```

.d8888b. 888 888      d8888 88888888 888b 888 .d8888b.
d88P Y88b 888 888      d88888 888 8888b 888 d88P Y88b
888 888 888 888      d88P888 888 88888b 888 Y88b.
888      88888888888 d88P 888 888 888Y88b 888 "Y888b.
888      888 888 d88P 888 888 888 Y88b888 "Y88b.
888 888 888 888 d88P 888 888 888 Y88888 "888
Y88b d88P 888 888 d88888888888 888 888 Y8888 Y88b d88P
"Y8888P" 888 888 d88P 888 88888888 888 Y888 "Y8888P"

```

CHAINS is a research project at [KTH Royal Institute of Technology](https://kth.se), it is about hardening the software supply chain, incl. dependency engineering as well as reproducible, executable and verifiable builds and SBOMs. We primarily look at Maven, NPM, and the software supply chain of crypto. The project is funded by the [Swedish Foundation for Strategic research \(SSF\)](https://ssf.se).

To get notified about project news, subscribe to the [Chains mailing list](#).

<https://chains.proj.kth.se/>





<NOT JUST DEPENDENCIES IN POM>

**<MAVEN-LOCKFILE ENABLES HERMETIC
BUILDS>**

<INVITING USERS AND CONTRIBUTORS>





/THANKS!

amansha@kth.se

bpimente@redhat.com

Link to GitHub repository:

<https://github.com/chains-project/maven-lockfile>

Link to demo:

<https://github.com/algomaster99/maven-hermeto-demo>



CREDITS: This presentation template was created by Slidesgo, and includes icon by Flaticon, and infographics & images by Freepik