# Vandmo Lock Plugin Information

### General Information (Taken from the github repository):

* Maven only requires you to specify versions of dependencies that you use directly. Transitive dependencies aren't visible in the pom.xml and their version is chosen in a seemingly random way.
* This Maven plugin enables you to:
  + Review exactly which dependencies you have, including transitive ones
  + Make sure dependencies are not accidentally changed
  + Verify the integrity of your dependencies to avoid supply chain attacks, see [Dependency Confusion](https://fossa.com/blog/dependency-confusion-understanding-preventing-attacks/)
  + Track changes to dependencies in your SCM
  + Enable vulnerability scanning in all your dependencies, including transitive ones
  + Enable Dependabot Security Alerts for transitive dependencies
* It is a bit like mvn dependency:list but the output is intended to be tracked by you SCM and the check goal makes sure you don't forget to update the file.

More information can be found on the Github repository:

<https://github.com/vandmo/dependency-lock-maven-plugin>

### Setup:

* If you change the pom you need to run the following command:
  + mvn se.vandmo:dependency-lock-maven-plugin:lock

### Potential Issues

Dependency Download Error:

You may run into the following warning after running the dependency lock command:



* This warning is related to a dependency not downloading correctly.
  + Warning can sometimes be ignored if the broken dependency has no transitive dependencies.
* The quick fix for it is to go into the .m2 folder & remote the broken dependency.
* You can also completely clean the .m2 folder & that will also likely fix it.

The dependency lock plugin also has various configuration settings that may be helpful for fixing issues related to this although I would highly recommend leaving it as it is and not using any configuration settings.

At the very least, you shouldn’t apply these configuration settings to all of the dependencies.

### Tips

Compare dependency-lock.json files between versions, double check that no dependencies are missing between upgrades. If you are missing dependencies, it's likely you missed the warning mentioned earlier & are missing transitive dependencies.

If you wanted to add a configuration setting to the plugin it would look like so:

A screen shot of a computer program

Description automatically generated

In this case the plugin is allowing extraneous dependencies on every dependency.