

goto;

GOTO Copenhagen 2023

#GOTOCph

Keep your dependencies in check

GOTO Copenhagen - Oct 2, 2023



<https://maritvandijk.com/>



@MaritvanDijk77



@MaritvanDijk77

**Friends: How did you write this
code so beautifully ?
Me(Proudly):**



@MaritvanDijk77

YO DAWG, I HEARD YOU LIKE DEPENDENCIES



imgflip.com

@MaritvanDijk77

VULNERABILITIES



@MaritvanDijk77

Dec. 2021

@MaritvanDijk77

**INFOSEC GETTING
READY FOR THE HOLIDAYS**



WELL IT'S LOG4J PATCH DAY

AGAIN

imgflip.com

@MaritvanDijk77

WE HAVE HAD ONE CVE, YES



BUT WHAT ABOUT A SECOND LOG4J CVE?

imgflip.com

@MaritvanDijk77

March 2022

@MaritvanDijk77



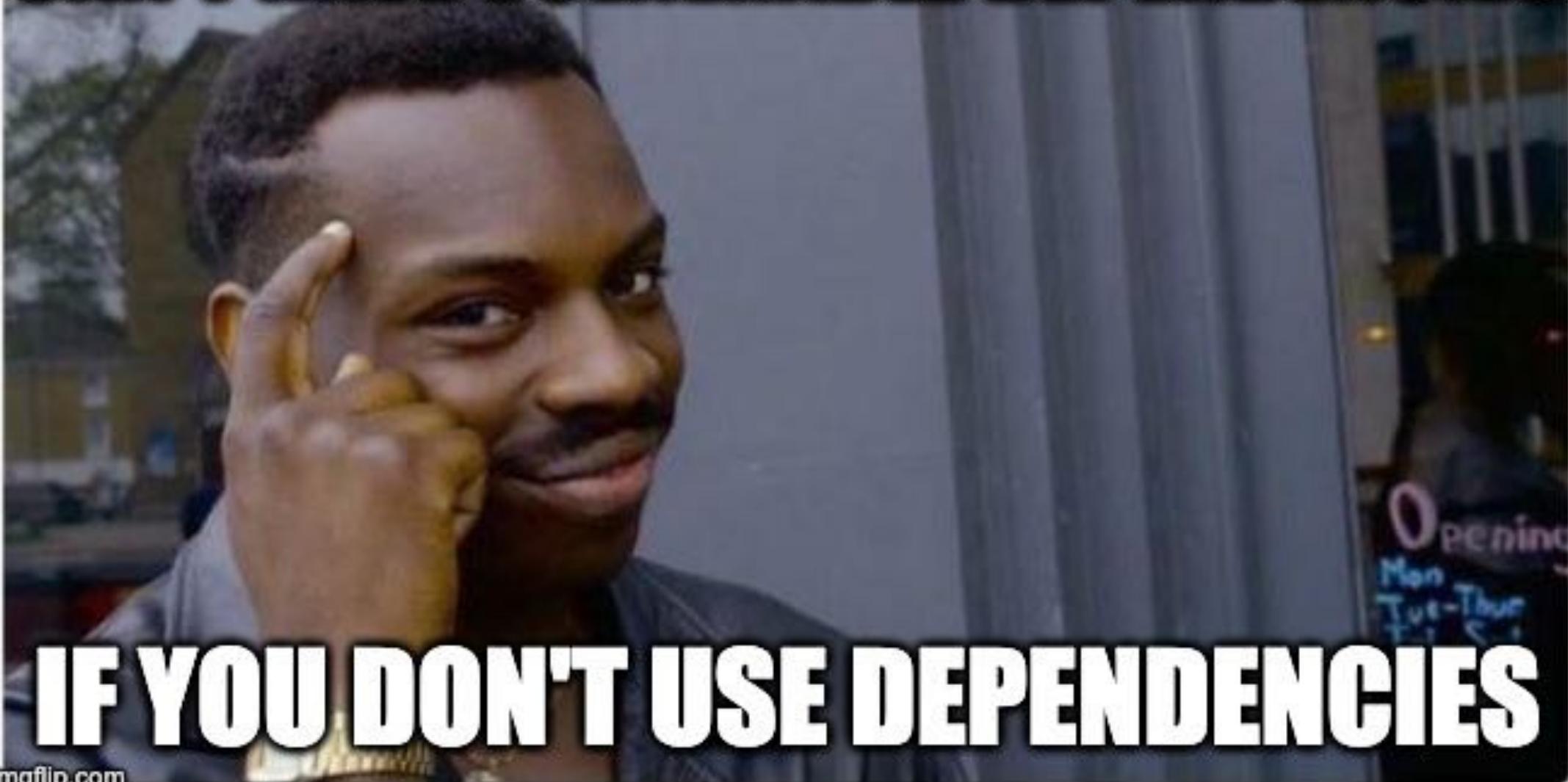
imgflip.com

@MaritvanDijk77



@MaritvanDijk77

CAN'T HAVE VULNERABLE DEPENDENCIES



USING



ALL THE DEPENDENCIES

@MaritvanDijk77

Do we
need
this
dependency?



@MaritvanDijk77

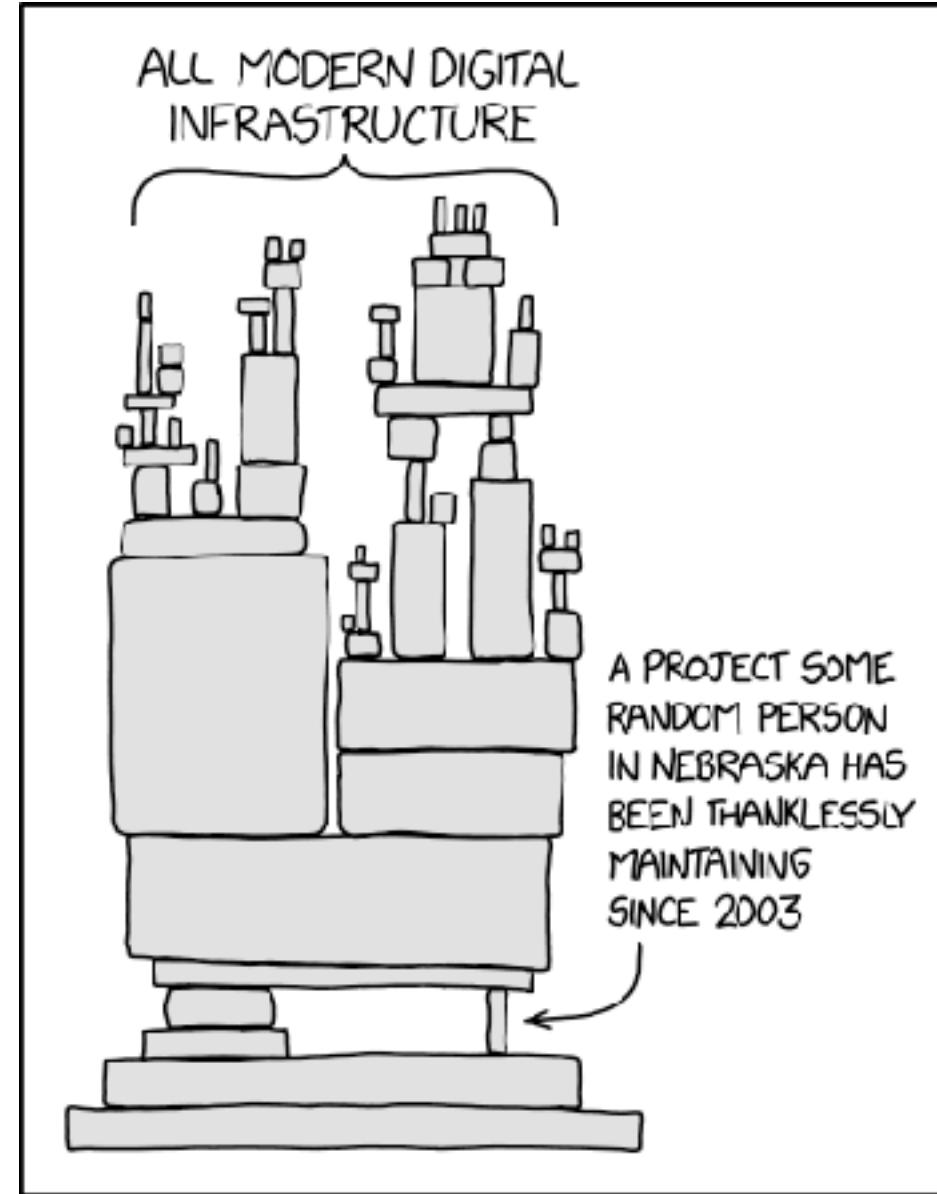
Selecting dependencies

@MaritvanDijk77

Selecting dependencies



@MaritvanDijk77



<https://xkcd.com/2347/>

@MaritvanDijk77

Selecting dependencies



@MaritvanDijk77

Selecting dependencies

@MaritvanDijk77

A close-up photograph of a dandelion seed head, showing its intricate structure of numerous small, white, feathery seeds radiating from a central brown stem. The background is dark and out of focus.

Selecting dependencies

@MaritvanDijk77

A close-up photograph of a weathered green wooden door. A metal chain with a padlock is attached to the door, symbolizing security or dependency. The door shows signs of age and wear.

Selecting dependencies

@MaritvanDijk77

Log4j download dashboard

log4j Latest Statistics

249,556,989

Total Downloads Since Dec 10, 2021

29 % vulnerable

23 %

Vulnerable Downloads Last 7 Days

3,490,799 total downloads

<https://www.sonatype.com/resources/log4j-vulnerability-resource-center>

@MaritvanDijk77

A magnifying glass with a black handle and a silver frame is positioned over a blue target symbol. The target has three concentric circles: a light blue outer ring, a medium blue middle ring, and a dark blue inner circle. The magnifying glass is focused directly on the center of the target's bullseye.

Find information

@MaritvanDijk77

Dependency information



Maven Central Repository Search

Quick Stats



Search



[Advanced Options](#) | [API Guide](#)

Official search by the maintainers of Maven Central Repository



Dependency information

Welcome!

On February 23, 2023, we started redirecting users from search.maven.org to central.sonatype.com. Launched in September of 2022, central.sonatype.com provides the main functionality of search.maven.org with enhanced search results, including security vulnerability and software quality information.

If you discover functionality that's missing or have suggestions for things to add, we'd love to hear from you, [so create an Improvement Issue in the MVNCENTRAL project](#).

[Click here to go back to search.maven.org](#), and we won't redirect you back here.

For more details on this change, please see [this FAQ on central.sonatype.org](#).

[Close](#)

Dependency information

The screenshot shows the Sonatype Maven Central Repository search interface. At the top left is the Sonatype logo and the text "maven central repository". At the top right are links for "API Doc", "Help", "Browse", and "Sign In". The main heading "Find OSS Components" is centered above a search bar containing the placeholder "Search". Below the search bar is a subtext: "As stewards of Central for nearly 20 years and inventors of both software supply chain management and Nexus Repository, Sonatype knows that the integrity of your build is critical."

sonatype | maven central repository

API Doc Help Browse Sign In

Find OSS Components

As stewards of Central for nearly 20 years and inventors of both software supply chain management and Nexus Repository, Sonatype knows that the integrity of your build is critical.

[Advanced Options](#)

<https://central.sonatype.com/>

@MaritvanDijk77

Dependency information

 sonatype | Maven Central Repository Search Quick Stats

com.fasterxml.jackson.core:jackson-databind:2.15.2



View on CGIndex

Browse Downloads

jackson-databind
General data-binding functionality for Jackson: Works on core streaming API

Licenses: The Apache Software License, Version 2.0
 Home page: <https://github.com/FasterXML/jackson>
 Source code: <https://github.com/FasterXML/jackson-databind>
 Inception year: 2008

com.fasterxml.jackson.core:jackson-databind
2.15.2

```
<!-- version="1.0" encoding="UTF-8"-->
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
<!-- This module was also published with a richer model. Gradle metadata. -->
<!-- which should be used instead. Do not delete the following line which -->
<!-- is an artifact to Gradle or any Gradle module metadata file consumers -->
<!-- that they should prefer consuming it instead. -->
<!-- do_not_use_as_an_artifact_published_with_gradle_metadata -->
modelVersion=0.9.0/modelVersion
parent:
  <groupId>com.fasterxml.jackson</groupId>
  <artifactId>jackson-core</artifactId>
  <version>2.14.2</version>
/>parent
<groupId>com.fasterxml.jackson.core</groupId>
<artifactId>jackson-databind</artifactId>
<version>2.15.2</version>
<name>jackson-databind</name>
<packaging>kotlin</packaging>
```

Apache Maven
maven.apache.org/

```
<dependency>
<groupId>com.fasterxml.jackson.core</groupId>
<artifactId>jackson-databind</artifactId>
<version>2.15.2</version>
</dependency>
```

Gradle Groovy DSL
gradle.org/

```
implementation "com.fasterxml.jackson.core:jackson-databind:2.15.2"
```

Gradle Kotlin DSL
github.com/gradle/kotlin-dsl

```
implementation("com.fasterxml.jackson.core:jackson-databind:2.15.2")
```

Scala SBT

[Search Maven Resources](#) | [About Sonatype](#) | [Privacy Policy](#) | [Terms Of Service](#) | [Get Support](#)

Copyright ©2023 Sonatype, Inc.

<https://search.maven.org/artifact/com.fasterxml.jackson.core:jackson-databind/2.15.2/jar>

@MaritvanDijk77

Dependency information

Sonatype | maven central repository Search

jackson-databind 2.15.2 ▼

Used in 42538 components

pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.15.2 Copy

[Overview](#) [Versions](#) [Dependents](#) [Dependencies](#)

Overview

General data-binding functionality for Jackson: works on core streaming API

Snippets

Apache Maven ▼ Copy to clipboard

```
<dependency>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <version>2.15.2</version>
</dependency>
```

Maven POM File

Copy to clipboard

Sonatype Safety Rating

An aggregate rating designed to represent a project's readiness against vulnerabilities.

5 out of 10 How did we get this score?

OSS Index

No vulnerabilities [View](#)

Metadata

4 months ago
Licenses
The Apache Software License, Version 2.0
12.3 kB

<https://central.sonatype.com/artifact/com.fasterxml.jackson.core/jackson-databind>

@MaritvanDijk77

Dependency information

 sonatype | OSS INDEX

[Search](#) [Ecosystems](#) [Integrations](#) [Documentation](#) [Who is Sonatype?](#) [Report a Vulnerability](#)

 [Sign In](#)

[« Back to Component Details](#)

jackson-databind

com.fasterxml.jackson.core

Version 2.15.2

 [Report advisory or correction](#)

Vulnerabilities

This version of jackson-databind has no known vulnerabilities! 🎉

@MaritvanDijk77

Dependency information

 sonatype | OSS INDEX

[Search](#) [Ecosystems](#) [Integrations](#) [Documentation](#) [Who is Sonatype?](#) [Report a Vulnerability](#)

 [Sign In](#)

[« Back to Component Details](#)

jackson-databind

com.fasterxml.jackson.core

Version 2.12.7

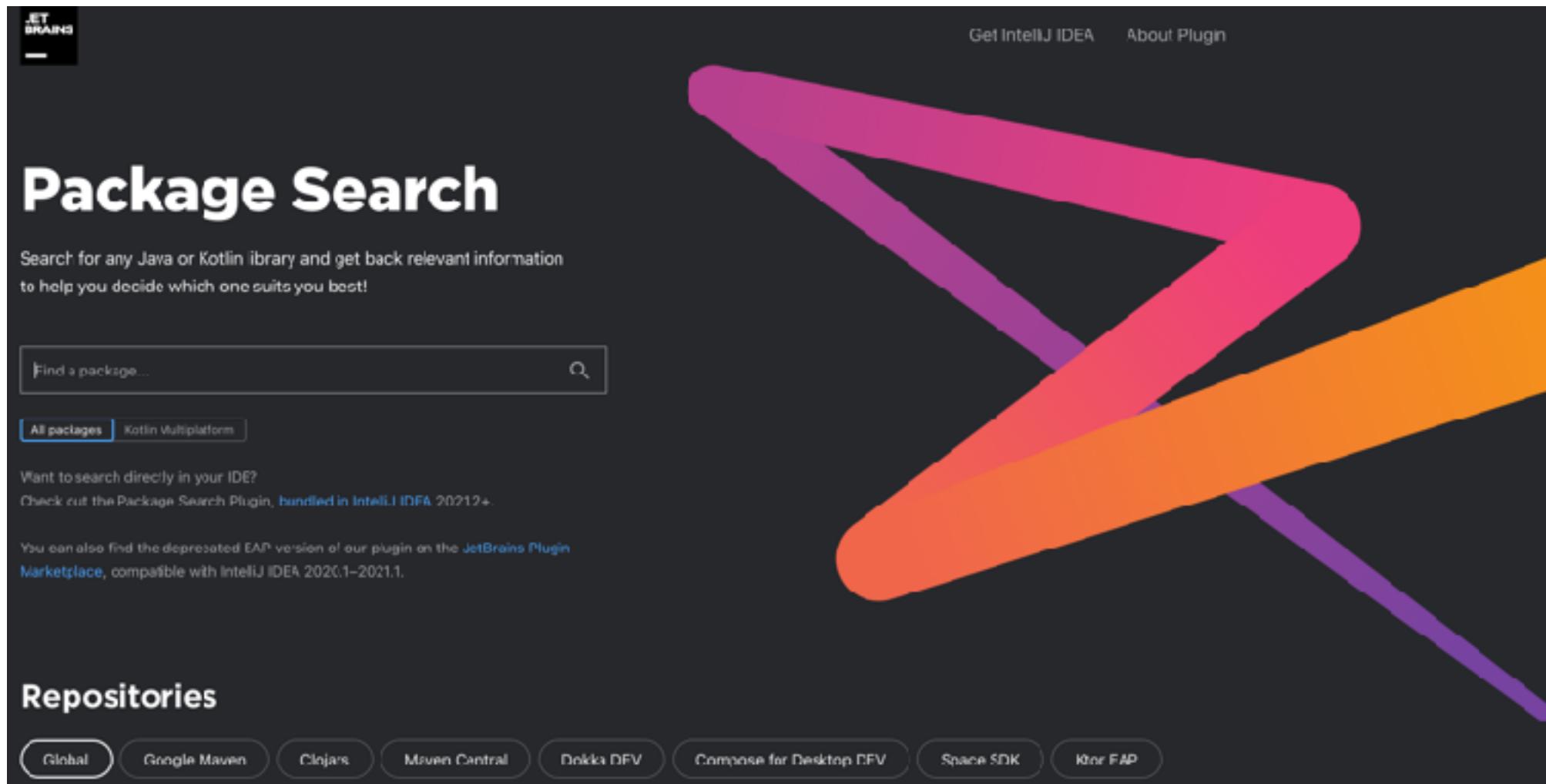
 [Report advisory or correction](#)

Vulnerabilities

2  HIGH

@MaritvanDijk77

Dependency information



A screenshot of the Package Search website. The page has a dark background with a large, stylized orange and purple swoosh graphic on the right side. At the top, there's a navigation bar with links for "Get IntelliJ IDEA" and "About Plugin". On the left, there's a search bar with placeholder text "Find a package..." and a magnifying glass icon. Below the search bar are two buttons: "All packages" (which is highlighted) and "Kotlin Multiplatform". A note below these buttons says "Want to search directly in your IDE? Check out the Package Search Plugin, bundled in IntelliJ IDEA 2021.4." Another note at the bottom says "You can also find the deprecated EAP version of our plugin on the [JetBrains Plugin Marketplace](#), compatible with IntelliJ IDEA 2020.1–2021.1." At the bottom, there's a section titled "Repositories" with several buttons for "Global", "Google Maven", "Clojars", "Maven Central", "Dokka DFV", "Compose for Desktop DFV", "Space SDK", and "Ktor EAP".

<https://package-search.jetbrains.com/>

@MaritvanDijk77

Dependency information



[Get IntelliJ IDEA](#) [About Plugin](#)

Find a package...



All packages

Kotlin Multiplatform

jackson-databind

com.fasterxml.jackson.core:
jackson-databind

[Information](#) [Readme](#) [Versions](#)

Latest version: 2.15.1

About package

Latest stable: 2.15.1

General data-binding functionality for Jackson: works on core streaming API

Updated on: May 17, 2023

The package is on GitHub, it has 3 313 stars, 168 watchers and has been forked 1 304 times.

StackOverflow: [core](#), [jackson-databind](#)

License: [Apache License 2.0](#)

Platforms: jvm

Add the package to your project

[Gradle \(Groovy\)](#) [Gradle \(Kotlin\)](#) [Maven](#) **SBT**

```
<dependency>
    <scope>compile</scope>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <version>2.15.1</version>
</dependency>
```

@MaritvanDijk77

Dependency information



JET BRAINS

Find a package... All packages Kotlin Multiplatform

Get IntelliJ IDEA About Plugin

jackson-databind

com.fasterxml.jackson.core:
jackson-databind

Information Readme Versions

Latest version: 2.15.1

Find a version

Stable

Latest stable: 2.15.1

Updated on: May 17, 2023

StackOverflow: [core, jackson-databind](#)

License: Apache License 2.0

Platforms: jvm

Authors: [Tatu Saloranta](#),
[Christopher Currie](#), [Paul Brown](#)

Package homepage on GitHub

Source code

Version	▲	Repositories	Last Updated	▼	Stable
2.15.1		Maven Central	May 17, 2023		✓
2.14.2		Maven Central	Jan 29, 2023		✓
2.13.5		Maven Central	Jan 23, 2023		✓
2.14.0		Maven Central	Nov 06, 2022		✓
2.14.0-rc3		Maven Central	Oct 28, 2022		—
2.13.4.2		Maven Central	Oct 19, 2022		✓

@MaritvanDijk77

Dependency information



FasterXML / jackson-databind

Type to search | [+ -](#) | [○](#) | [n](#)

[Code](#) [Issues 477](#) [Pull requests 26](#) [Discussions](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#)

jackson-databind Public

[Sponsor](#) [Watch 167](#) [Fork 1.3k](#) [Star 3.4k](#)

2.16 · 27 branches · 187 tags

Go to file Add file ▾ < Code ▾

cowtowncoder	A further tweak to handle a corner case of #3647	1 ✓ b2ab29c 5 hours ago	7,209 commits
.github	Bump actions/checkout from 4.0.0 to 4.1.0 (#4126)	5 days ago	
.mvn/wrapper	Merge branch '2.15' into 2.16	3 months ago	
attic	Clean up attic...	5 months ago	
docs	Add javadoc redirects	9 months ago	
release-notes	Update release notes wrt #3647 fix	8 hours ago	
src	A further tweak to handle a corner case of #3647	5 hours ago	
.gitattributes	Merge branch '2.7' into 2.8	7 years ago	
.gitignore	minor Ignorai cleanup	6 years ago	
LICENSE	Add full LICENSE at main level (backport from master)	3 years ago	

About

General data-binding package for Jackson (2.x): works on streaming API (core) implementation(s)

json jackson hacktoberfest
jackson-databind

[Readme](#) [Apache-2.0 license](#) [Security policy](#) [Activity](#) [3.4k stars](#) [167 watching](#) [1.3k forks](#)

[Report repository](#)

<https://github.com/>

@MaritvanDijk77

Dependency information



FasterXML / jackson-databind

Type ⌘ to search

Code Issues 477 Pull requests 26 Discussions Actions Projects Wiki Security Insights

- Pulse
- Contributors
- Community Standards
- Commits
- Code frequency
- Dependency graph
- Network
- Forks

September 24, 2023 – October 1, 2023

Period: 1 week ▾

Overview

9 Active pull requests

7 Active issues

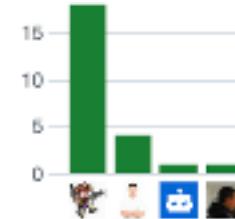
8 Merged pull requests

1 Open pull request

7 Closed issues

0 New issues

Excluding merges, 4 authors have pushed 19 commits to 2.16 and 24 commits to all branches. On 2.16, 23 files have changed and there have been 755 additions and 77 deletions.

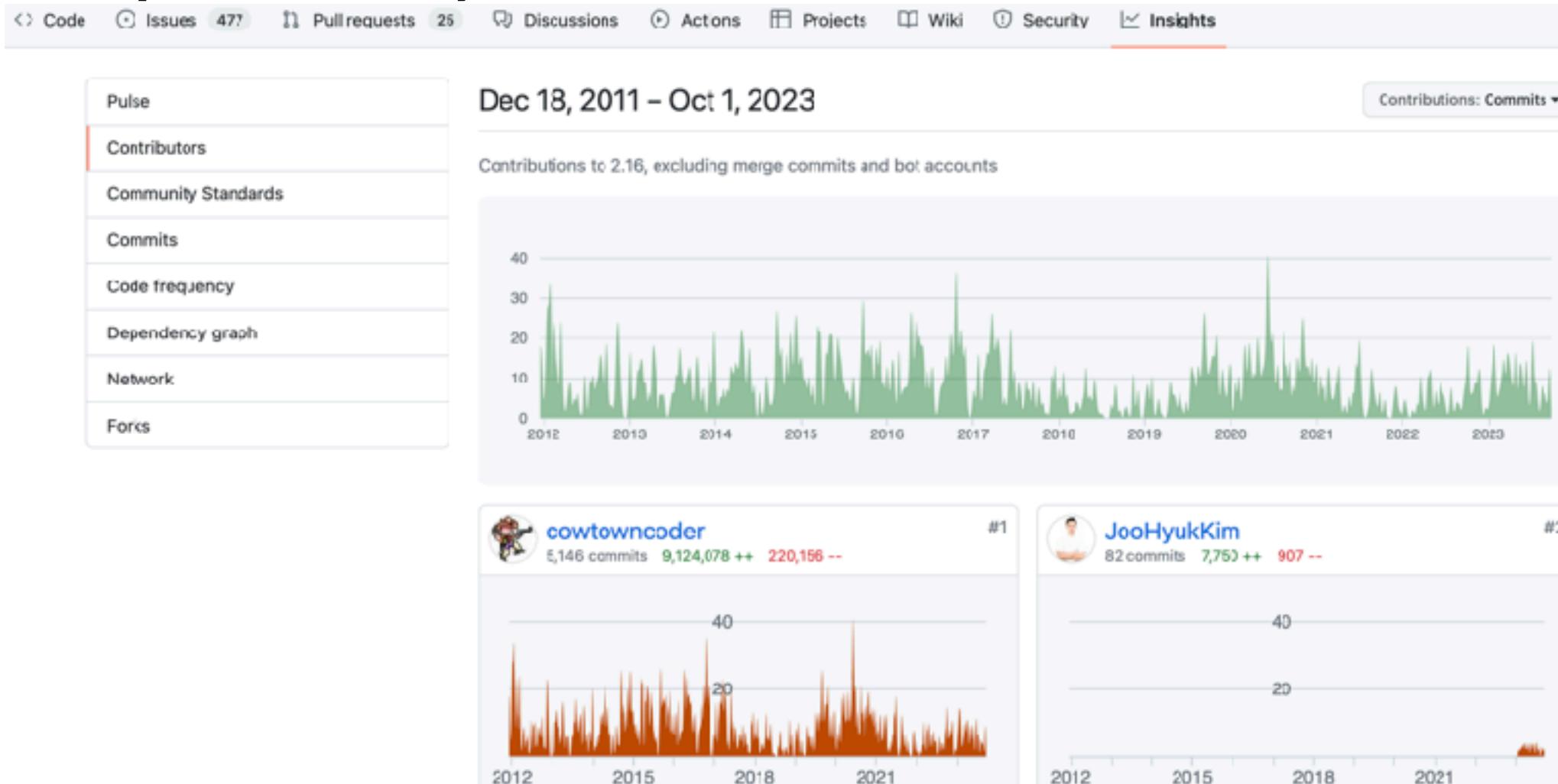


8 Pull requests merged by 4 people

<https://github.com/>

@MaritvanDijk77

Dependency information



<https://github.com/>

@MaritvanDijk77



imgflip.com

Maintain dependencies



@MaritvanDijk77

Maven

- Overview of dependencies: `mvn dependency:tree`

```
marit.van.dijk@NV000260 FitnessTracker % ./mvnw dependency:tree
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ FitnessTracker ---
[INFO] com.maritvandijk:FitnessTracker:war:1.0-SNAPSHOT
[INFO] +- junit:junit:jar:3.8.1:compile
[INFO] +- org.springframework:spring-webmvc:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-aop:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-beans:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-context:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-core:jar:4.3.5.RELEASE:compile
[INFO] |   |   \- commons-logging:commons-logging:jar:1.2:compile
[INFO] |   +- org.springframework:spring-expression:jar:4.3.5.RELEASE:compile
[INFO] |   \- org.springframework:spring-web:jar:4.3.5.RELEASE:compile
```

Maven

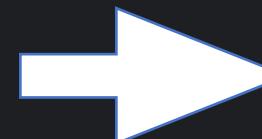
- Check for updates: `mvn versions:display-dependency-updates`

```
marit.van.dijk@NVC00260 FitnessTracker % mvn versions:display-dependency-updates
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- versions-maven-plugin:2.13.0:display-dependency-updates (default-cli) @ FitnessTracker ---
[INFO] The following dependencies in Dependencies have newer versions:
[INFO]   com.fasterxml.jackson.core:jackson-annotations ..... 2.9.7 -> 2.15.2
[INFO]   com.fasterxml.jackson.core:jackson-core ..... 2.9.7 -> 2.15.2
[INFO]   com.fasterxml.jackson.core:jackson-databind ..... 2.9.7 -> 2.15.2
[INFO]   com.thoughtworks.xstream:xstream ..... 1.4.18 -> 1.4.20
[INFO]   javax.servlet:servlet-api ..... 2.5 -> 3.8-alpha-1
[INFO]   junit:junit ..... 3.8.1 -> 4.13.2
[INFO]   org.hibernate:hibernate-validator ..... 4.2.0.Final -> 8.0.0.Final
[INFO]   org.springframework:spring-oxm ..... 4.3.5.RELEASE -> 6.0.9
[INFO]   org.springframework:spring-webmvc ..... 4.3.5.RELEASE -> 6.0.9
[INFO]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```

Maven

- Check for updates: `mvn versions:display-dependency-updates`

```
marit.van.dijk@NVC06260 FitnessTracker % ./mvnw versions:display-dependency-updates
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- versions-maven-plugin:2.13.0:display-dependency-updates (default-cli) @ FitnessTracker ---
[INFO] The following dependencies in Dependencies have newer versions:
[INFO]   com.fasterxml.jackson.core:jackson-annotations ..... 2.9.7 -> 2.15.0
[INFO]   com.fasterxml.jackson.core:jackson-core ..... 2.9.7 -> 2.15.0
[INFO]   com.fasterxml.jackson.core:jackson-databind ..... 2.9.7 -> 2.15.0
[INFO]   com.thoughtworks.xstream:xstream ..... 1.4.19 -> 1.4.20
[INFO]   javax.servlet:servlet-api ..... 2.5 -> 3.8-alpha-1
[INFO]   junit:junit ..... 3.8.1 -> 4.13.2
[INFO]   org.hibernate:hibernate-validator ..... 4.2.0.Final -> 8.0.0.Final
[INFO]   org.springframework:spring-oxm ..... 4.3.5.RELEASE -> 6.0.8
[INFO]   org.springframework:spring-webmvc ..... 4.3.5.RELEASE -> 6.0.8
[INFO]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```



2.15.0-rc2
2.15.0-rc1
2.14.2
2.13.5
2.14.1

@MaritvanDijk77

Maven

- Analyze dependencies: `mvn dependency:analyze`

```
[INFO] --- maven-dependency-plugin:2.8:analyze (default-cli) @ FitnessTracker ---
[WARNING] Used undeclared dependencies found:
[WARNING]   org.springframework:spring-beans:jar:4.3.5.RELEASE:compile
[WARNING]   org.springframework:spring-web:jar:4.3.5.RELEASE:compile
[WARNING]   javax.validation:validation-api:jar:1.0.0.GA:compile
[WARNING]   org.springframework:spring-context:jar:4.3.5.RELEASE:compile
[WARNING] Unused declared dependencies found:
[WARNING]   junit:junit:jar:3.8.1:compile
[WARNING]   org.springframework:spring-webmvc:jar:4.3.5.RELEASE:compile
[WARNING]   javax.servlet:servlet-api:jar:2.5:provided
[WARNING]   javax.servlet:jstl:jar:1.2:provided
[WARNING]   com.fasterxml.jackson.core:jackson-core:jar:2.9.7:compile
[WARNING]   com.fasterxml.jackson.core:jackson-annotations:jar:2.9.7:compile
[WARNING]   com.fasterxml.jackson.core:jackson-databind:jar:2.9.7:compile
[WARNING]   com.thoughtworks.xstream:xstream:jar:1.4.10:compile
[WARNING]   org.springframework:spring-oxm:jar:4.3.5.RELEASE:compile
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```

Gradle

- Overview of dependencies: `./gradlew dependencies`

```
aotCompileClasspath - Compile classpath for source set 'aot'.
+--- org.springframework.boot:spring-boot-starter-cache -> 3.1.0
|   +--- org.springframework.boot:spring-boot-starter:3.1.0
|   |   +--- org.springframework.boot:spring-boot:3.1.0
|   |   |   +--- org.springframework:spring-core:6.0.9
|   |   |   |   \--- org.springframework:spring-jcl:6.0.9
|   |   |   \--- org.springframework:spring-context:6.0.9
|   |   |   +--- org.springframework:spring-aop:6.0.9
|   |   |   |   +--- org.springframework:spring-beans:6.0.9
|   |   |   |   |   \--- org.springframework:spring-core:6.0.9 (*)
|   |   |   |   \--- org.springframework:spring-core:6.0.9 (*)
|   |   +--- org.springframework:spring-beans:6.0.9 (*)
|   |   +--- org.springframework:spring-core:6.0.9 (*)
|   |   \--- org.springframework:spring-expression:6.0.9
|       \--- org.springframework:spring-core:6.0.9 (*)
+--- org.springframework.boot:spring-boot-autoconfigure:3.1.0
|   \--- org.springframework.boot:spring-boot:3.1.0 (*)
+--- org.springframework.boot:spring-boot-starter-logging:3.1.0
|   +--- ch.qos.logback:logback-classic:1.4.7
```



Gradle

- Check for updates:
- Add plugin, e.g. gradle-versions-plugin

```
plugins {  
    id 'java'  
    id 'com.github.ben-manes.versions' version '0.48.0'  
}
```

- Run `./gradlew dependencyUpdates`

```
The following dependencies have later milestone versions:  
- com.github.ben-manes.caffeine:caffeine [3.1.6 -> 3.1.8]  
  https://github.com/ben-manes/caffeine  
- com.h2database:h2 [2.1.214 -> 2.2.224]  
  https://h2database.com
```



Gradle

- Analyze dependencies
- Add plugin (e.g. nebula)

[nebula-plugins / gradle-lint-plugin](#) Public

Code Issues 97 Pull requests 6 Actions Projects Wiki Security Insights

Unused Dependency Rule

Jon Schneider edited this page on Sep 22, 2016 - 4 revisions

The unused dependency rule is an example of a complex dependency hygiene rule.

To apply the rule, add:

```
gradleLint.rules += 'unused-dependency'
```

The rule inspects compiled binaries emanating from your project's [source sets](#) looking for class references, and matches those references to the dependencies that you have declared in your [dependencies](#) block.

Specifically, the rule makes the following adjustments to dependencies:

1. Removes unused dependencies
 - Family-style jars like `com.amazonaws:aws-java-sdk` are removed, as they contain no code
2. Promotes transitive dependencies that are used directly by your code to explicit first order dependencies
 - This has the side effect of breaking up family style jars like `com.amazonaws:aws-java-sdk` into the parts that you are actually using, and adding those as first order dependencies
3. Relocates dependencies to the 'correct' configuration

<https://github.com/nebula-plugins/gradle-lint-plugin/wiki/Unused-Dependency-Rule>

@MaritvanDijk77



Gradle

- Analyze dependencies
- Add plugin (e.g. nebula)
- Run `./gradlew fixGradleLint`

```
buildscript { repositories { mavenCentral() } }
plugins {
    id 'nebula.lint' version '18.1.0'
}
gradleLint.rules = ['all-dependency']
```

```
> Task :fixGradleLint
```

```
This project contains lint violations. A complete listing of my attempt to fix them follows. Please review and commit the changes.
```

```
needs fixing  unused-dependency          one or more classes in org.springframework.data:spring-data-commons:3.1.1 are required by your code directly
needs fixing  unused-dependency          this dependency should be removed since its artifact is empty
build.gradle:42
testImplementation 'org.springframework.boot:spring-boot-starter-test'

fixed        unused-dependency          this dependency is unused and can be removed
```



IntelliJ IDEA: View Dependencies

The screenshot shows the IntelliJ IDEA interface with the Maven tool window open. The left pane displays the `pom.xml` file, specifically the `<dependencies>` section. This section lists various Spring and Spring Boot dependencies, including `spring-boot-starter-actuator`, `spring-boot-starter-cache`, `spring-boot-starter-data-jpa`, `spring-boot-starter-web`, `spring-boot-starter-validation`, and `spring-boot-starter-thymeleaf`. The right pane shows the dependency tree, with nodes for each dependency and their transitive dependencies.

```
spring-petclinic > pom.xml (spring-petclinic) >
  28  <dependencies>
  29    <!-- Spring and Spring Boot dependencies -->
  30  40    <dependency>
  31    41      <groupId>org.springframework.boot</groupId>
  32    42      <artifactId>spring-boot-starter-actuator</artifactId>
  33    43    </dependency>
  34    44    <dependency>
  35    45      <groupId>org.springframework.boot</groupId>
  36    46      <artifactId>spring-boot-starter-cache</artifactId>
  37    47    </dependency>
  38    48    <dependency>
  39    49      <groupId>org.springframework.boot</groupId>
  40    50      <artifactId>spring-boot-starter-data-jpa</artifactId>
  41    51    </dependency>
  42    52    <dependency>
  43    53      <groupId>org.springframework.boot</groupId>
  44    54      <artifactId>spring-boot-starter-web</artifactId>
  45    55    </dependency>
  46    56    <dependency>
  47    57      <groupId>org.springframework.boot</groupId>
  48    58      <artifactId>spring-boot-starter-validation</artifactId>
  49    59    </dependency>
  50    60    <dependency>
  51    61      <groupId>org.springframework.boot</groupId>
  52    62      <artifactId>spring-boot-starter-thymeleaf</artifactId>
  53    63    </dependency>
  54    64    <dependency>
  55    65
  56    66
  57    67
  58    68
  59    69
  60    70
  61    71
  62    72
  63    73
  64    74
  65    75
  66    76
  67    77
  68    78
  69    79
  70    80
  71    81
  72    82
  73    83
  74    84
  75    85
  76    86
  77    87
  78    88
  79    89
  80    90
  81    91
  82    92
  83    93
  84    94
  85    95
  86    96
  87    97
  88    98
  89    99
  90    100
  91    101
  92    102
  93    103
  94    104
  95    105
  96    106
  97    107
  98    108
  99    109
  100  110
  101  111
  102  112
  103  113
  104  114
  105  115
  106  116
  107  117
  108  118
  109  119
  110  120
  111  121
  112  122
  113  123
  114  124
  115  125
  116  126
  117  127
  118  128
  119  129
  120  130
  121  131
  122  132
  123  133
  124  134
  125  135
  126  136
  127  137
  128  138
  129  139
  130  140
  131  141
  132  142
  133  143
  134  144
  135  145
  136  146
  137  147
  138  148
  139  149
  140  150
  141  151
  142  152
  143  153
  144  154
  145  155
  146  156
  147  157
  148  158
  149  159
  150  160
  151  161
  152  162
  153  163
  154  164
  155  165
  156  166
  157  167
  158  168
  159  169
  160  170
  161  171
  162  172
  163  173
  164  174
  165  175
  166  176
  167  177
  168  178
  169  179
  170  180
  171  181
  172  182
  173  183
  174  184
  175  185
  176  186
  177  187
  178  188
  179  189
  180  190
  181  191
  182  192
  183  193
  184  194
  185  195
  186  196
  187  197
  188  198
  189  199
  190  200
  191  201
  192  202
  193  203
  194  204
  195  205
  196  206
  197  207
  198  208
  199  209
  200  210
  201  211
  202  212
  203  213
  204  214
  205  215
  206  216
  207  217
  208  218
  209  219
  210  220
  211  221
  212  222
  213  223
  214  224
  215  225
  216  226
  217  227
  218  228
  219  229
  220  230
  221  231
  222  232
  223  233
  224  234
  225  235
  226  236
  227  237
  228  238
  229  239
  230  240
  231  241
  232  242
  233  243
  234  244
  235  245
  236  246
  237  247
  238  248
  239  249
  240  250
  241  251
  242  252
  243  253
  244  254
  245  255
  246  256
  247  257
  248  258
  249  259
  250  260
  251  261
  252  262
  253  263
  254  264
  255  265
  256  266
  257  267
  258  268
  259  269
  260  270
  261  271
  262  272
  263  273
  264  274
  265  275
  266  276
  267  277
  268  278
  269  279
  270  280
  271  281
  272  282
  273  283
  274  284
  275  285
  276  286
  277  287
  278  288
  279  289
  280  290
  281  291
  282  292
  283  293
  284  294
  285  295
  286  296
  287  297
  288  298
  289  299
  290  300
  291  301
  292  302
  293  303
  294  304
  295  305
  296  306
  297  307
  298  308
  299  309
  300  310
  301  311
  302  312
  303  313
  304  314
  305  315
  306  316
  307  317
  308  318
  309  319
  310  320
  311  321
  312  322
  313  323
  314  324
  315  325
  316  326
  317  327
  318  328
  319  329
  320  330
  321  331
  322  332
  323  333
  324  334
  325  335
  326  336
  327  337
  328  338
  329  339
  330  340
  331  341
  332  342
  333  343
  334  344
  335  345
  336  346
  337  347
  338  348
  339  349
  340  350
  341  351
  342  352
  343  353
  344  354
  345  355
  346  356
  347  357
  348  358
  349  359
  350  360
  351  361
  352  362
  353  363
  354  364
  355  365
  356  366
  357  367
  358  368
  359  369
  360  370
  361  371
  362  372
  363  373
  364  374
  365  375
  366  376
  367  377
  368  378
  369  379
  370  380
  371  381
  372  382
  373  383
  374  384
  375  385
  376  386
  377  387
  378  388
  379  389
  380  390
  381  391
  382  392
  383  393
  384  394
  385  395
  386  396
  387  397
  388  398
  389  399
  390  400
  391  401
  392  402
  393  403
  394  404
  395  405
  396  406
  397  407
  398  408
  399  409
  400  410
  401  411
  402  412
  403  413
  404  414
  405  415
  406  416
  407  417
  408  418
  409  419
  410  420
  411  421
  412  422
  413  423
  414  424
  415  425
  416  426
  417  427
  418  428
  419  429
  420  430
  421  431
  422  432
  423  433
  424  434
  425  435
  426  436
  427  437
  428  438
  429  439
  430  440
  431  441
  432  442
  433  443
  434  444
  435  445
  436  446
  437  447
  438  448
  439  449
  440  450
  441  451
  442  452
  443  453
  444  454
  445  455
  446  456
  447  457
  448  458
  449  459
  450  460
  451  461
  452  462
  453  463
  454  464
  455  465
  456  466
  457  467
  458  468
  459  469
  460  470
  461  471
  462  472
  463  473
  464  474
  465  475
  466  476
  467  477
  468  478
  469  479
  470  480
  471  481
  472  482
  473  483
  474  484
  475  485
  476  486
  477  487
  478  488
  479  489
  480  490
  481  491
  482  492
  483  493
  484  494
  485  495
  486  496
  487  497
  488  498
  489  499
  490  500
  491  501
  492  502
  493  503
  494  504
  495  505
  496  506
  497  507
  498  508
  499  509
  500  510
  501  511
  502  512
  503  513
  504  514
  505  515
  506  516
  507  517
  508  518
  509  519
  510  520
  511  521
  512  522
  513  523
  514  524
  515  525
  516  526
  517  527
  518  528
  519  529
  520  530
  521  531
  522  532
  523  533
  524  534
  525  535
  526  536
  527  537
  528  538
  529  539
  530  540
  531  541
  532  542
  533  543
  534  544
  535  545
  536  546
  537  547
  538  548
  539  549
  540  550
  541  551
  542  552
  543  553
  544  554
  545  555
  546  556
  547  557
  548  558
  549  559
  550  560
  551  561
  552  562
  553  563
  554  564
  555  565
  556  566
  557  567
  558  568
  559  569
  560  570
  561  571
  562  572
  563  573
  564  574
  565  575
  566  576
  567  577
  568  578
  569  579
  570  580
  571  581
  572  582
  573  583
  574  584
  575  585
  576  586
  577  587
  578  588
  579  589
  580  590
  581  591
  582  592
  583  593
  584  594
  585  595
  586  596
  587  597
  588  598
  589  599
  590  600
  591  601
  592  602
  593  603
  594  604
  595  605
  596  606
  597  607
  598  608
  599  609
  600  610
  601  611
  602  612
  603  613
  604  614
  605  615
  606  616
  607  617
  608  618
  609  619
  610  620
  611  621
  612  622
  613  623
  614  624
  615  625
  616  626
  617  627
  618  628
  619  629
  620  630
  621  631
  622  632
  623  633
  624  634
  625  635
  626  636
  627  637
  628  638
  629  639
  630  640
  631  641
  632  642
  633  643
  634  644
  635  645
  636  646
  637  647
  638  648
  639  649
  640  650
  641  651
  642  652
  643  653
  644  654
  645  655
  646  656
  647  657
  648  658
  649  659
  650  660
  651  661
  652  662
  653  663
  654  664
  655  665
  656  666
  657  667
  658  668
  659  669
  660  670
  661  671
  662  672
  663  673
  664  674
  665  675
  666  676
  667  677
  668  678
  669  679
  670  680
  671  681
  672  682
  673  683
  674  684
  675  685
  676  686
  677  687
  678  688
  679  689
  680  690
  681  691
  682  692
  683  693
  684  694
  685  695
  686  696
  687  697
  688  698
  689  699
  690  700
  691  701
  692  702
  693  703
  694  704
  695  705
  696  706
  697  707
  698  708
  699  709
  700  710
  701  711
  702  712
  703  713
  704  714
  705  715
  706  716
  707  717
  708  718
  709  719
  710  720
  711  721
  712  722
  713  723
  714  724
  715  725
  716  726
  717  727
  718  728
  719  729
  720  730
  721  731
  722  732
  723  733
  724  734
  725  735
  726  736
  727  737
  728  738
  729  739
  730  740
  731  741
  732  742
  733  743
  734  744
  735  745
  736  746
  737  747
  738  748
  739  749
  740  750
  741  751
  742  752
  743  753
  744  754
  745  755
  746  756
  747  757
  748  758
  749  759
  750  760
  751  761
  752  762
  753  763
  754  764
  755  765
  756  766
  757  767
  758  768
  759  769
  760  770
  761  771
  762  772
  763  773
  764  774
  765  775
  766  776
  767  777
  768  778
  769  779
  770  780
  771  781
  772  782
  773  783
  774  784
  775  785
  776  786
  777  787
  778  788
  779  789
  780  790
  781  791
  782  792
  783  793
  784  794
  785  795
  786  796
  787  797
  788  798
  789  799
  790  800
  791  801
  792  802
  793  803
  794  804
  795  805
  796  806
  797  807
  798  808
  799  809
  800  810
  801  811
  802  812
  803  813
  804  814
  805  815
  806  816
  807  817
  808  818
  809  819
  810  820
  811  821
  812  822
  813  823
  814  824
  815  825
  816  826
  817  827
  818  828
  819  829
  820  830
  821  831
  822  832
  823  833
  824  834
  825  835
  826  836
  827  837
  828  838
  829  839
  830  840
  831  841
  832  842
  833  843
  834  844
  835  845
  836  846
  837  847
  838  848
  839  849
  840  850
  841  851
  842  852
  843  853
  844  854
  845  855
  846  856
  847  857
  848  858
  849  859
  850  860
  851  861
  852  862
  853  863
  854  864
  855  865
  856  866
  857  867
  858  868
  859  869
  860  870
  861  871
  862  872
  863  873
  864  874
  865  875
  866  876
  867  877
  868  878
  869  879
  870  880
  871  881
  872  882
  873  883
  874  884
  875  885
  876  886
  877  887
  878  888
  879  889
  880  890
  881  891
  882  892
  883  893
  884  894
  885  895
  886  896
  887  897
  888  898
  889  899
  890  900
  891  901
  892  902
  893  903
  894  904
  895  905
  896  906
  897  907
  898  908
  899  909
  900  910
  901  911
  902  912
  903  913
  904  914
  905  915
  906  916
  907  917
  908  918
  909  919
  910  920
  911  921
  912  922
  913  923
  914  924
  915  925
  916  926
  917  927
  918  928
  919  929
  920  930
  921  931
  922  932
  923  933
  924  934
  925  935
  926  936
  927  937
  928  938
  929  939
  930  940
  931  941
  932  942
  933  943
  934  944
  935  945
  936  946
  937  947
  938  948
  939  949
  940  950
  941  951
  942  952
  943  953
  944  954
  945  955
  946  956
  947  957
  948  958
  949  959
  950  960
  951  961
  952  962
  953  963
  954  964
  955  965
  956  966
  957  967
  958  968
  959  969
  960  970
  961  971
  962  972
  963  973
  964  974
  965  975
  966  976
  967  977
  968  978
  969  979
  970  980
  971  981
  972  982
  973  983
  974  984
  975  985
  976  986
  977  987
  978  988
  979  989
  980  990
  981  991
  982  992
  983  993
  984  994
  985  995
  986  996
  987  997
  988  998
  989  999
  990  1000
```



IntelliJ IDEA: View Dependencies

```
spring-petclinic | ② versions | ⌂
```

```
build.gradle (spring-petclinic) | ②
```

```
18 ext.webjarsFontawesomeVersion = "4.7.0"
```

```
19 ext.webjarsBootstrapVersion = "5.2.3"
```

```
20
```

```
21
```

```
22 dependencies {
```

```
23     implementation 'org.springframework.boot:spring-boot-starter-cache'
```

```
24     implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
```

```
25     implementation 'org.springframework.boot:spring-boot-starter-thymeleaf'
```

```
26     implementation 'org.springframework.boot:spring-boot-starter-web'
```

```
27     implementation 'org.springframework.boot:spring-boot-starter-validation'
```

```
28     implementation 'javax.cache:cache-api'
```

```
29     implementation 'jakarta.xml.bind:jakarta.xml.bind-api'
```

```
30     runtimeOnly 'org.springframework.boot:spring-boot-starter-actuator'
```

```
31     runtimeOnly 'org.webjars.npm:bootstrap:${webjarsBootstrapVersion}'
```

```
32     runtimeOnly 'org.webjars.npm:font-awesome:${webjarsFontawesomeVersion}'
```

```
33     runtimeOnly 'com.github.ben-manes.caffeine:caffeine'
```

```
34     runtimeOnly 'com.h2database:h2'
```

```
35     runtimeOnly 'com.mysql:mysql-connector-j'
```

```
36     runtimeOnly 'org.postgresql:postgresql'
```

```
37     developmentOnly 'org.springframework.boot:spring-boot-devtools'
```

```
38     testImplementation 'org.springframework.boot:spring-boot-starter-test'
```

```
39 }
```

```
40
```

```
41 tasks.named("test") {
```

```
42     useJUnitPlatform()
```

```
43 }
```

```
44
```

```
plugins()
```

6:54 LF UTF-8 4 spaces

@MaritvanDijk77

IntelliJ IDEA: View Dependencies



The screenshot shows the IntelliJ IDEA interface with two main windows. On the left is the 'Project' tool window, which displays a tree view of the project structure. A red box highlights the 'External Libraries' node, indicating the focus of the tutorial. On the right is the code editor window showing the contents of the build.gradle file for the 'spring-petclinic' project. The code lists various dependencies and build tasks, including Spring Boot starters, Jakarta XML Bindings, and specific database connectors like H2 and MySQL.

```
ext.webjarsFontawesomeVersion = "4.7.0"
ext.webjarsBootstrapVersion = "5.2.3"

dependencies {
    implementation 'org.springframework.boot:spring-boot-starter-cache'
    implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
    implementation 'org.springframework.boot:spring-boot-starter-thymeleaf'
    implementation 'org.springframework.boot:spring-boot-starter-web'
    implementation 'org.springframework.boot:spring-boot-starter-validation'
    implementation 'javax.cache:cache-api'
    implementation 'jakarta.xml.bind:jakarta.xml.bind-api'
    runtimeOnly 'org.springframework.boot:spring-boot-starter-actuator'
    runtimeOnly 'org.webjars.npm:bootstrap:${webjarsBootstrapVersion}'
    runtimeOnly 'org.webjars.npm:font-awesome:${webjarsFontawesomeVersion}'
    runtimeOnly 'com.github.ben-manes.caffeine:caffeine'
    runtimeOnly 'com.h2database:h2'
    runtimeOnly 'com.mysql:mysql-connector-j'
    runtimeOnly 'org.postgresql:postgresql'
    developmentOnly 'org.springframework.boot:spring-boot-devtools'
    testImplementation 'org.springframework.boot:spring-boot-starter-test'
}

tasks.named('test') {
    useJUnitPlatform()
}
```



IntelliJ IDEA: View Dependencies

The screenshot shows two panels in IntelliJ IDEA. On the left is the code editor displaying the `pom.xml` file for the project `spring-petclinic`. The right panel is the `Maven` tool window, which displays a tree view of dependencies. A red box highlights the `Dependencies` node under the project node. The dependency tree includes:

- `org.springframework.boot:spring-boot-starter-actuator`
- `org.springframework.boot:spring-boot-starter-cache`
- `org.springframework.boot:spring-boot-starter-data-jpa`
- `org.springframework.boot:spring-boot-starter-web`
- `org.springframework.boot:spring-boot-starter-validation`
- `org.springframework.boot:spring-boot-starter-thymeleaf`
- `org.springframework.boot:spring-boot-starter-test`
- `com.h2database:h2` (runtime)
- `com.mysql:mysql-connector-j` (runtime)
- `org.postgresql:postgresql` (runtime)
- `javassist:javassist`

<https://www.jetbrains.com/help/idea/maven-projects-tool-window.html>

@MaritvanDijk77





IntelliJ IDEA: View Dependencies



The screenshot shows the IntelliJ IDEA interface. On the left, the code editor displays the `build.gradle` file for a Spring Boot application named `spring-petclinic`. The file contains dependencies for various Spring Boot starters and external libraries like Caffeine and MySQL connector. On the right, the `Gradle` tool window is open, showing the dependency tree for the project. A red box highlights the `Dependencies` section, which lists all the dependencies declared in the `build.gradle` file, including their versions and transitive dependencies.

```
spring-petclinic -> build.gradle (spring-petclinic) <--> gradle
```

```
ext.webjarsFontawesomeVersion = "4.7.0"
ext.webjarsBootstrapVersion = "5.2.3"

dependencies {
    implementation 'org.springframework.boot:spring-boot-starter-cache'
    implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
    implementation 'org.springframework.boot:spring-boot-starter-thymeleaf'
    implementation 'org.springframework.boot:spring-boot-starter-web'
    implementation 'org.springframework.boot:spring-boot-starter-validation'
    implementation 'javax.cache:cache-api'
    implementation 'jakarta.xml.bind:jakarta.xml.bind-api'
    runtimeOnly 'org.springframework.boot:spring-boot-starter-actuator'
    runtimeOnly 'org.webjars.npm:bootstrap:=${webjarsBootstrapVersion}'
    runtimeOnly 'org.webjars.npm:font-awesome:${webjarsFontawesomeVersion}'
    runtimeOnly 'com.github.ben-manes.caffeine:caffeine'
    runtimeOnly 'com.h2database:h2'
    runtimeOnly 'com.mysql:mysql-connector-j'
    runtimeOnly 'org.postgresql:postgresql'
    developmentOnly 'org.springframework.boot:spring-boot-devtools'
    testImplementation 'org.springframework.boot:spring-boot-starter-test'
}

tasks.named('test') {
    useJUnitPlatform()
}
```

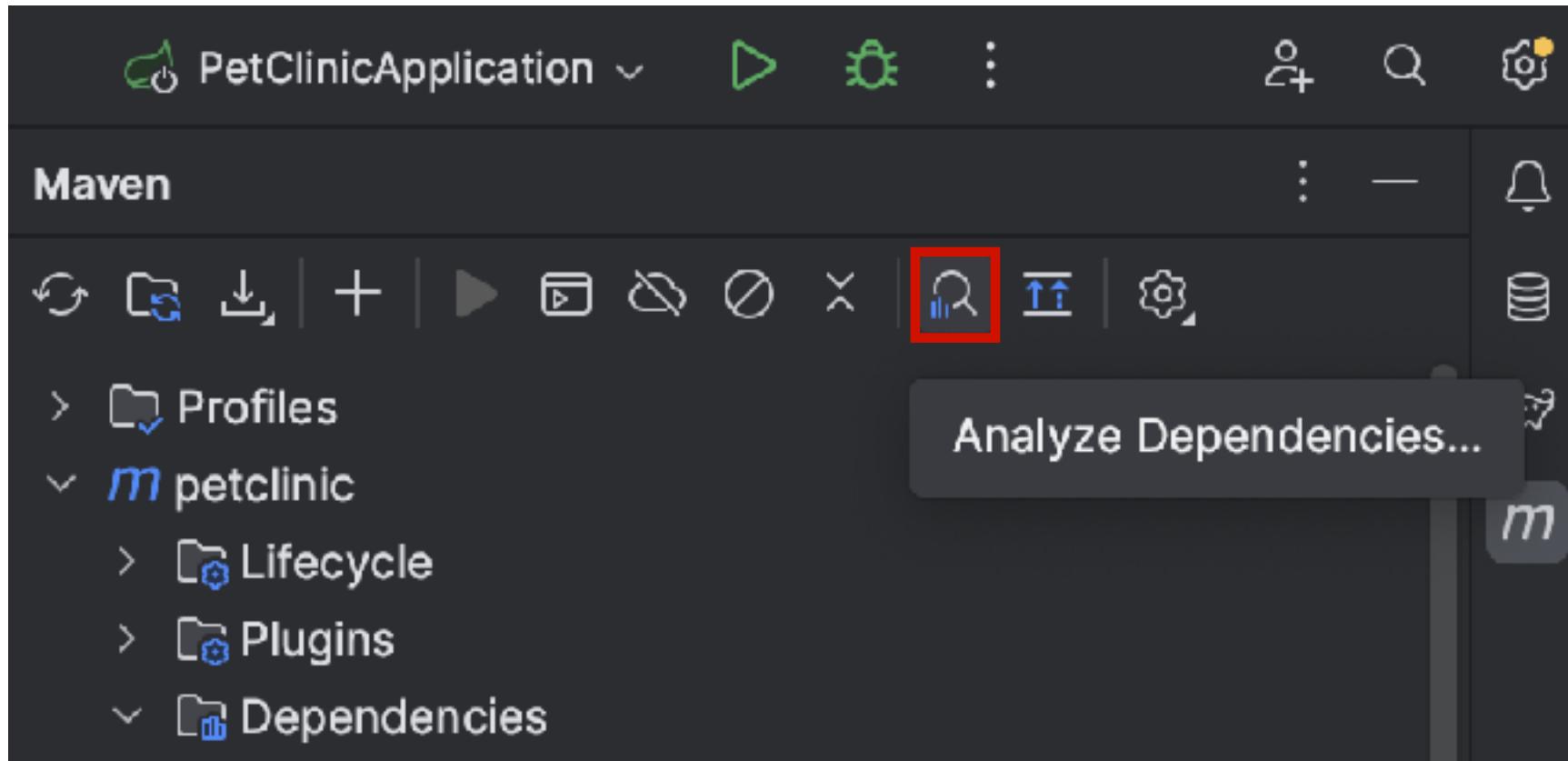
Gradle

- spring-petclinic
- Tasks
- Dependencies
 - actCompileClasspath
 - amClasses
 - com.github.ben-manes.caffeine:caffeine:3.1.6
 - com.h2database:h2:2.2.1.214
 - com.mysql:mysql-connector-j:8.0.33
 - jakarta.xml.bind:jakarta.xml.bind-api:4.0.0 (*)
 - jevex.cache:cache-api:1.1.1
 - main
 - main
 - org.postgresql:postgresql:42.8.0
 - org.springframework.boot:spring-boot-starter-actuator
 - org.springframework.boot:spring-boot-starter-ci
 - org.springframework.boot:spring-boot-starter-data-jpa
 - org.springframework.boot:spring-boot-starter-thymeleaf
 - org.springframework.boot:spring-boot-starter-web
 - org.apache.tomcat.embed:tomcat-embed-el
 - org.hibernate.validator.hibernate-validator:8.0.1.Final
 - com.fasterxml.jackson.core:jackson-databind:2.13.0
 - jakarta.validation:jakarta.validation-api:3.0.0
 - org.jboss.logging:jboss-logging:3.5.0.Final
 - org.springframework.boot:spring-boot-starter-data-jpa
 - org.springframework.boot:spring-boot-starter-web
 - org.webjars.npm:bootstrap:5.2.3

<https://www.jetbrains.com/help/idea/jetgradle-tool-window.html>

@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer



https://www.jetbrains.com/help/idea/work-with-maven-dependencies.html#dependency_analyzer

@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer

A screenshot of the IntelliJ IDEA interface showing the "Dependency Analyzer" tool window. The window has two main panes. The left pane, titled "Resolved Dependencies", lists various dependencies with their coordinates and scopes. The right pane, titled "Usages of assertj-core:3.24.2", shows the specific usages of this dependency within the project. A search bar at the top of the window allows for filtering dependencies by name.

spring-petclinic

petclinic

Resolved Dependencies

petclinic (compile)

accessors-smart:2.4.9 (test)

android-json:0.0.20131108.vaadin1 (test)

angus-activation:2.0.0 (runtime)

antlr4-runtime:4.10.1 (compile)

apiguardian-api:1.1.2 (test)

asm:9.3 (test)

aspectjweaver:1.9.19 (compile)

assertj-core:3.24.2 (test)

PetClinicApplication

Usages of assertj-core:3.24.2

petclinic (compile)

spring-boot-starter-test:3.1.0 (test)

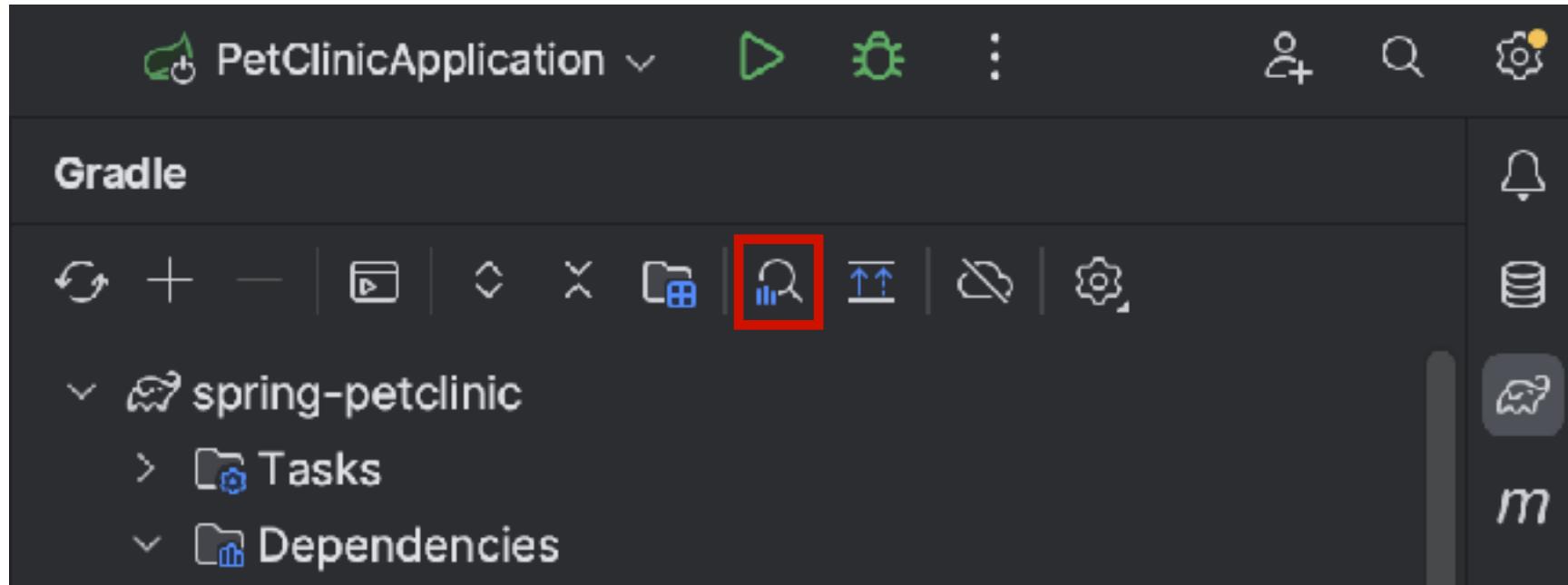
assertj-core:3.24.2 (test)

https://www.jetbrains.com/help/idea/work-with-maven-dependencies.html#dependency_analyzer

@MaritvanDijk77

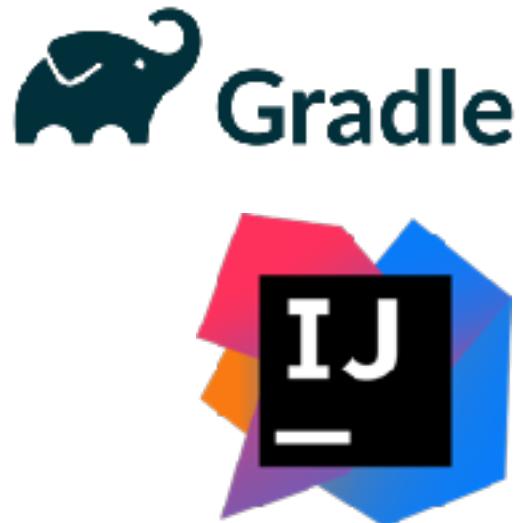


IntelliJ IDEA: Dependency Analyzer



https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

@MaritvanDijk77



IntelliJ IDEA: Dependency Analyzer

The screenshot shows the IntelliJ IDEA interface with the 'Dependency Analyzer' tool window open. The search bar at the top of the window has 'spring' typed into it, which is highlighted with a red box. To the right of the search bar is a 'Scope: Any' dropdown and a clear button. Below the search bar, the left panel displays a tree view of resolved dependencies for the 'spring-petclinic' project, including 'spring-petclinic (3 scopes)', 'spring-aop:6.0.9 (13 scopes)', 'spring-aspects:6.0.9 (12 scopes)', 'spring-beans:6.0.9 (13 scopes)', and 'spring-boot-actuator-autoconfigure:3.1.0 (10 scopes)'. The right panel shows the 'Usages of spring-petclinic' section, which includes a tree view of usage locations for 'spring-petclinic' across three scopes.

https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

@MaritvanDijk77



IntelliJ IDEA: Dependency Analyzer

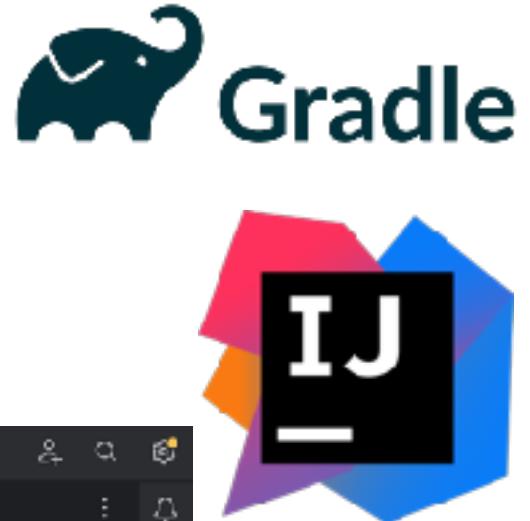
The screenshot shows the IntelliJ IDEA interface with the "Dependency Analyzer" tab selected. On the left, a tree view lists "Resolved Dependencies" for the project "spring-petclinic". Some nodes are expanded to show their scope (e.g., "spring-petclinic (3 scopes)", "accessors-smart:2.4.9 (5 scopes)"). On the right, a "Scope" dropdown menu is open, displaying a list of available scopes. The "Any" scope is currently selected. Other scopes listed include AnnotationProcessor, ActAnnotationProcessor, ActCompileClasspath, ActRuntimeClasspath, ActTestAnnotationProcessor, ActTestCompileClasspath, ActTestRuntimeClasspath, Archives, CompileClasspath, Default, DevelopmentOnly, NetliveImageClasspath, NetliveImageTestClasspath, ProcessActClasspath, ProcessTestActClasspath, ProductionRuntimeClasspath, RuntimeClasspath, TestAnnotationProcessor, TestCompileClasspath, and TestRuntimeClasspath.

- Scope: Any ▾
- Any
- AnnotationProcessor
- ActAnnotationProcessor
- ActCompileClasspath
- ActRuntimeClasspath
- ActTestAnnotationProcessor
- ActTestCompileClasspath
- ActTestRuntimeClasspath
- Archives
- CompileClasspath
- Default
- DevelopmentOnly
- NetliveImageClasspath
- NetliveImageTestClasspath
- ProcessActClasspath
- ProcessTestActClasspath
- ProductionRuntimeClasspath
- RuntimeClasspath
- TestAnnotationProcessor
- TestCompileClasspath
- TestRuntimeClasspath

https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

@MaritvanDijk77





IntelliJ IDEA: Dependency Analyzer

A screenshot of the IntelliJ IDEA interface, specifically the "Dependency Analyzer" tool window. The window shows a tree view of resolved dependencies for a project named "spring-petclinic". The root node is "checker-qual:3.33.0" (10 scopes). Below it, under "spring-petclinic (default)", are "spring-petclinic (2 scopes)" and "caffeine:3.1.6 (2 scopes)". The "caffeine" node has a child "checker-qual:3.33.0 (2 scopes) conflict with 3.31.0". Further down the tree are "postgresql:42.6.0 (2 scopes)", "caffeine:3.1.6 (6 scopes)", "postgresql:42.6.0 (8 scopes)", "spring-boot-dependencies:3.1.0 (2 scopes)", "caffeine:3.1.6 (2 scopes)", and "postgresql:42.6.0 (2 scopes)". The "checker-qual" nodes under "postgresql" and "spring-boot-dependencies" also show conflicts with version 3.31.0. The "Dependency Analyzer" tab is selected in the top navigation bar. A red box highlights the "Scopes: Any" dropdown menu, which is open, showing options like "Show Conflicts Only".

- checker-qual:3.33.0 (10 scopes)
- junit-bom:5.9.3 (4 scopes)
- spring-petclinic (default)
 - spring-petclinic (2 scopes)
 - caffeine:3.1.6 (2 scopes)
 - checker-qual:3.33.0 (2 scopes) conflict with 3.31.0
- postgresql:42.6.0 (2 scopes)
 - checker-qual:3.33.0 (2 scopes) conflict with 3.31.0
- caffeine:3.1.6 (6 scopes)
 - checker-qual:3.33.0 (6 scopes) conflict with 3.31.0
- postgresql:42.6.0 (8 scopes)
 - checker-qual:3.33.0 (8 scopes) conflict with 3.31.0
- spring-boot-dependencies:3.1.0 (2 scopes)
 - caffeine:3.1.6 (2 scopes)
 - checker-qual:3.33.0 (2 scopes) conflict with 3.31.0
- postgresql:42.6.0 (2 scopes)
 - checker-qual:3.33.0 (2 scopes) conflict with 3.31.0

https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

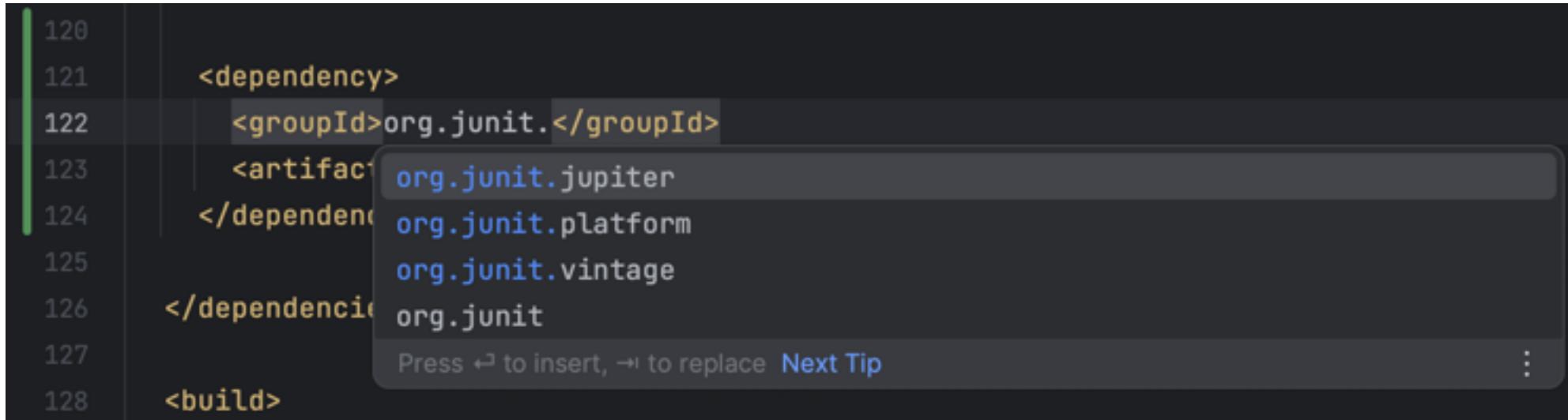
@MaritvanDijk77

IntelliJ IDEA

Maven™



- Package Search: Add dependency



A screenshot of the IntelliJ IDEA code editor showing a Maven XML configuration file. The cursor is positioned at the start of the 'groupId' tag for a dependency. A tooltip is displayed, listing several artifact IDs that match the partial text 'org.junit.jupiter'. The listed artifacts include 'org.junit.jupiter', 'org.junit.platform', 'org.junit.vintage', and 'org.junit'. Below the list, there is a message: 'Press ⇧ to insert, ⌘ to replace' followed by a 'Next Tip' link. The code editor has a dark theme with syntax highlighting for XML tags and attributes.

```
120
121      <dependency>
122          <groupId>org.junit.</groupId>
123          <artifactId>org.junit.jupiter
124      </dependency>
125      <dependency>org.junit.platform
126          <artifactId>org.junit.vintage
127      </dependency>
128      <dependency>org.junit
```

IntelliJ IDEA

Maven™



- Package Search: Add dependency

```
120
121      <dependency>
122          <groupId>org.junit.jupiter</groupId>
123          <artifactId>junit-jupiter</artifactId>
124          💡 <scope>test</scope>
125      </dependency>
```



IntelliJ IDEA: Update dependencies

- Context Actions (or Alt+Enter)

A screenshot of the IntelliJ IDEA interface showing a context menu over a portion of a Maven XML configuration file. The file contains code for dependency management, specifically for Spring Web MVC and JSTL. A context menu is open, listing several options:

- Change maven:org.springframework:spring-webmvc:4.3.5.RELEASE version to 6.0.0
- Show vulnerability info for maven:org.springframework:spring-beans:4.3.5.RELEASE
- Show vulnerability info for maven:org.springframework:spring-context:4.3.5.RELEASE
- Show vulnerability info for maven:org.springframework:spring-core:4.3.5.RELEASE
- Show vulnerability info for maven:org.springframework:spring-expression:4.3.5.RELEASE
- Show vulnerability info for maven:org.springframework:spring-web:4.3.5.RELEASE
- Show vulnerability info for maven:org.springframework:spring-webmvc:4.3.5.RELEASE

Below these, there are additional general context actions:

- Convert tag to attribute
- Convert text to CDATA
- Merge tags
- Split current tag
- Inject language or reference

At the bottom of the menu, it says "Press F1 to toggle preview".





IntelliJ IDEA: Update dependencies

- Hover

The screenshot shows a portion of a Maven `pom.xml` file on the left and its analysis results on the right. The code includes dependencies for Spring Framework and javax.servlet. A tooltip is displayed over the Spring dependency entry, listing four vulnerabilities found in version 4.3.5.RELEASE:

- CVE-2016-1000027 9.8 Deserialization of Untrusted Data vulnerability with high severity found
- CVE-2020-5397 5.3 Cross-Site Request Forgery (CSRF) vulnerability pending CVSS allocation
- CVE-2018-1271 5.9 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability pending CVSS allocation
- CVE-2018-11040 7.5 Inclusion of Functionality from Untrusted Control Sphere vulnerability pending CVSS allocation

Results powered by Checkmarx(c)

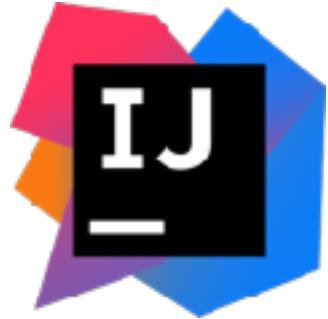
Change maven:org.springframework:spring-webmvc:4.3.5.RELEASE version to 6.0. More actions... More

Property
springframework.version: 4.3.5.RELEASE

Fitness Tracker

```
<groupId>org.springframework</groupId>
<artifactId>spring-webmvc</artifactId>
<version>${springframework.version}</version>
<scope>compile</scope>
</dependency>
<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>servlet-api</artifactId>
    <version>2.5</version>
    <scope>provided</scope>
</dependency>
<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>jstl</artifactId>
    <version>1.2</version>
    <scope>provided</scope>
</dependency>
```

IntelliJ IDEA



- Dependencies tool window

The screenshot shows the IntelliJ IDEA interface with the 'Dependencies' tool window open. The 'Manage' tab is selected. In the left sidebar, 'All Modules' is chosen, and the 'FitnessTracker' module is selected. The main pane displays a list of dependencies, with 'Jackson-annotations' highlighted. A detailed view of this dependency is shown on the right side of the window.

Dependency	Version	Upgrades
Jackson-annotations com.fasterxml.jackson.core:jackson-annotations [default] ~	2.9.7	→ 2.15.1 ✓ Upgrade...
Jackson-core com.fasterxml.jackson.core:jackson-core [default] ~	2.9.7	→ 2.14.2 ✓ Upgrade...
com.fasterxml.jackson.core:jackson-databind [default] ~	2.9.7	→ 2.15.1 ✓ Upgrade...
XStream Core com.thoughtworks.xstream:xstream [default] ~	1.4.10	→ 1.4.20 ✓ Upgrade...
javax.servlet:jstl	provided	✓
JavaServlet(TM) Specification javax.servlet:servlet	provided	✓
JUnit junit:junit	[default] ~	3.8.1 → 4.13.2 ✓ Upgrade...
Hibernate Validator Engine - Relocation Artifact	[default] ~	4.2.0.Final → 8.0.0 Upgrade...
Spring Object/XML Marshalling org.springframework:spring-object	[default] ~	4.3.5.RELEASE → ! Upgrade...
Spring Web MVC org.springframework:spring-webmvc	compile	4.3.5.RELEASE → ! Upgrade...

Jackson-annotations Upgrade

com.fasterxml.jackson.core:jackson-annotations

Core annotations used for value types, used by Jackson data binding package.

GitHub star 0

License: Apache License 2.0

Project site

Used in:

- * FitnessTracker

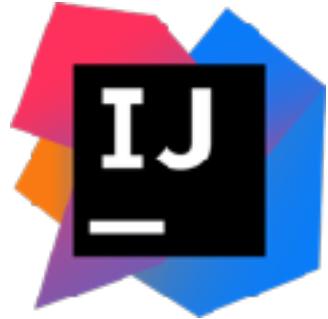
Authors: Tatu Saloranta, Christopher Currie, Paul Brown

18:21 LF UTF-8 4 spaces

<https://www.jetbrains.com/help/idea/package-search.html>

@MaritvanDijk77

IntelliJ IDEA



- Dependencies tool window (search)

The screenshot shows the IntelliJ IDEA interface with the 'Dependencies' tool window open. The 'Manage' tab is selected. In the left sidebar, 'All Modules' is chosen, and under it, the 'FitnessTracker' module is listed. A search bar at the top contains the text 'junit'. Below the search bar, there are two checkboxes: 'Only stable' (which is checked) and 'Kotlin multiplatform' (which is unchecked). The search results table has columns for 'Search Results' (25), 'Version', 'Upgrade all (1)', and 'Add'. The first result, 'JUnit junit:junit', is highlighted. To the right of the table, a detailed view for 'JUnit' is shown, including its description ('JUnit is a unit testing framework for Java, created by Erich Gamma and Kent Beck.'), GitHub link ('GitHub'), license information ('License: Eclipse Public License 1.0'), project site ('Project site'), documentation ('Documentation'), and a 'Readme' section. At the bottom of this panel, it says 'Used in:' followed by a list containing 'FitnessTracker'. The status bar at the bottom right shows the time as 18:21, file encoding as LF, character encoding as UTF-8, and code style as 4 spaces.

Search Results	Version	Upgrade all (1)	Add
JUnit junit:junit	[default] 3.8.1 → 4.13.2	Upgrade...	Add
JUnit junit:junit-dep	[default] 4.11		Add
org.junit-pioneer:junit-pioneer	[default] 2.0.0		Add
com.jcovalet.junit:jcovalet-junit-logging	[default] 0.1.1		Add
org.junit.contrib:junit-theories	[default] 5.0-alpha-3		Add
JUnit Rules com.btmattewson:junit:junit-rules	[default] 1.0.1		Add
JUnit Jupiter (Aggregator) org.junit.jupiter:junit	[default] 5.9.2		Add
JUnit Extensions org.dmonix:junit:junit-extensio	[default] 1.1		Add
ZooKeeper JUnit org.dmonix:junit:zookeeper-ju	[default] 1.2		Add
Junit Validation com.lotaris:junit:junit-validation	[default] 0.3.1		Add
org.fingerprintsoft:junit:junit-utils	[default] 1.4.0		Add
JUnit Categories net.ggttools:junit:junit-categor	[default] 1.0		Add

<https://www.jetbrains.com/help/idea/package-search.html>

@MaritvanDijk77

IntelliJ IDEA



Dependency Checker Vulnerable Dependencies

All libs from FitnessTracker

- maven:com.thoughtworks.xstream:xstream:2.3.1
- maven:com.fasterxml.jackson.core:jackson-databind:2.9.7**
- maven:org.springframework:spring-context:5.1.9.RELEASE
- maven:org.springframework:spring-beans:4.3.19.RELEASE
- maven:org.hibernate:hibernate-validator:4.2.0.Final
- maven:org.springframework:spring-webmv:2.5.6
- maven:org.springframework:spring-express:2.5.6

Dependency maven:com.fasterxml.jackson.core:jackson-databind:2.9.7 is vulnerable Results powered by Checkmarx

Upgrade to 2.12.7.1 Copy safe version to clipboard

H CVE-2019-16942, Score: 9.8

A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.7.9.7, 2.8x before 2.8.11.5 and 2.9.x before 2.9.10.1. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of

19:21 LF UTF-8 4 spaces ⌂

<https://www.jetbrains.com/help/idea/package-analysis.html>

@MaritvanDijk77

IntelliJ IDEA



IntelliJ IDEA: Viewing Dependencies



IntelliJ IDEA: Managing Dependencies



IntelliJ IDEA Ultimate: Package
Checker



IntelliJ IDEA: Analyzing
Dependencies



<https://www.youtube.com/@intellijidea>

@MaritvanDijk77

Pros & Cons

- + Check dependencies while working on the project
- Check out each individual project
- Apply & verify updates

Software Composition Analysis (SCA)

- Scan all repos (and containers)
- Overview



SCA: Pros & Cons

- + No need to check out repos individually
- I have to check the dashboard
- Apply & verify updates



Bots

Dependabot

Renovate

Snyk Open Source



@MaritvanDijk77

Dependabot



- GitHub native
- Features:
 - Alerts
 - Security updates
 - Version updates

@MaritvanDijk77

Dependabot enable



Settings

Pages

Saved replies

Security

Code security and analysis

Integrations

Applications

Scheduled reminders

Archives

Security log

Sponsorship log

Developer settings

Dependency graph

Understand your dependencies.

Automatically enable for new private repositories

Disable all

Enable all

Dependabot

Keep your dependencies secure and up-to-date. [Learn more about Dependabot](#).

Dependabot alerts

Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications](#).

Automatically enable for new repositories

Disable all

Enable all

Dependabot security updates

Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

Automatically enable for new repositories ✓

Disable all

Enable all

@MaritvanDijk77

Dependabot alerts



mlvandijk / FitnessTracker Public

Code Issues 1 Pull requests 53 Actions Security 90 Insights Settings

Pulse Contributors Community Community Standards Traffic Commits Code frequency Dependency graph

Dependencies Dependents Dependabot

⚠ We found potential security vulnerabilities in your dependencies.

Dependencies defined in these manifest files have known security vulnerabilities and should be updated:

pom.xml 90 vulnerabilities found

[View Dependabot alerts](#)

Only the owner of this repository can see this message.

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77

Dependabot alerts



Code Issues 1 Pull requests 62 Actions Security 91 Insights Settings

Pulse Contributors Community Community Standards Traffic Commits Code frequency Dependency graph Network Forks

Dependency graph

Dependencies Dependents Dependabot Export SBOM

Q Search all dependencies

com.fasterxml.jackson.core:jackson-databind 2.9.7 ④ 14 critical

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

com.thoughtworks.xstream:xstream 1.4.10 ④ 1 critical

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · NOASSERTION

org.springframework:spring-webmvc 4.3.5.RELEASE ④ 1 critical

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

<https://docs.github.com/en/code-security/dependabot/about-dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77

Dependabot alerts



Contributors

Community

Community Standards

Traffic

Commits

Code frequency

Dependency graph

Network

Forks

Dependencies Dependents Dependabot Export SBOM

Search all dependencies

com.fasterxml.jackson.core:jackson-databind 2.9.7 14 critical

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

com.thoughtworks.xstream:xstream 1.4.10

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · NOASSERTION

org.springframework:spring-webmvc 4.3.5.RELEASE

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

org.hibernate:hibernate-validator 4.2.0

Detected automatically on Feb 14, 2023 (Maven) · pom.xml

View Dependabot alerts
14 critical · 55 total

Update to v2.12.7.1
#70

pom.xml update suggested:
com.fasterxml.jackson... Open

Always verify the validity and compatibility of suggestions with your codebase.

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77

Dependabot security updates



Dependabot alerts / #85

Deserialization of untrusted data in FasterXML jackson-databind #85

[Dismiss alert ▾](#)

! Open

Opened 7 months ago on com.fasterxml.jackson.core:jackson-databind (Maven) · pom.xml

fix Bump jackson-databind from 2.9.7 to 2.12.7.1

Merging this pull request would fix 55 Dependabot alerts on com.fasterxml.jackson.core:jackson-databind in [pom.xml](#).

fix Review security update

Severity

Critical 9.8 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1|AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weaknesses

CWE-915
CWE-1321

! fix dependabot bot opened this 7 months ago

<https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/about-dependabot-security-updates>

@MaritvanDijk77

Dependabot security updates



> Code Issues 1 Pull requests 52 Actions Security 91 Insights Settings

Bump jackson-databind from 2.9.7 to 2.12.7.1 #70

Open dependabot wants to merge 1 commit into `main` from `dependabot/maven/com.fasterxml.jackson.core:jackson-databind-2.12.7.1`

Info Merging this pull request will resolve 55 Dependabot alerts on com.fasterxml.jackson.core:jackson-databind including a critical severity alert.

Conversation 1 Commits 1 Checks 0 Files changed 1 +1 -1

dependabot (bot) commented on behalf of github on Nov 16, 2022 · edited

Bumps jackson-databind from 2.9.7 to 2.12.7.1.

► Commits

Reviewers
No reviews
Still in progress? Convert to draft

<https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/about-dependabot-security-updates>

@MaritvanDijk77

Dependabot version updates



- Add dependabot.yml
- Specify:
 - Package manager & location of manifest file
 - Schedule interval (daily, weekly, or monthly)
- Optional:
 - Max. number of PR's (default 5)
 - Rebase strategy
 - Etc

<https://docs.github.com/en/code-security/dependabot/dependabot-version-updates/about-dependabot-version-updates>

@MaritvanDijk77

Dependabot: Supported platforms



- GitHub native
- Can run on GitLab too

@MaritvanDijk77

Renovate



- Available via GitHub App
- Features:
 - Security updates
 - Version updates
 - Project dashboard

Renovate enable



GitHub App

Renovate



Configure

Manage your installation settings.



Developer

 renovatebot

 Website

Renovate is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

 Report abuse

<https://github.com/apps/renovate>

@MaritvanDijk77

Renovate enable - 3



Install Renovate

Install on your personal account Marit van Dijk

All repositories
This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).

Only select repositories
Select at least one repository.
Also includes public repositories (read-only).

Select repositories ▾

Selected 1 repository.

mlvandijk/FitnessTracker x

@MaritvanDijk77

Renovate onboarding PR

Configure Renovate #59

[Open](#) renovate wants to merge 1 commit into `main` from `renovate/configure`

Conversation 0 Commits 1 Checks 0 Files changed 1

renovate commented 3 minutes ago

Welcome to [Renovate](#)! This is an onboarding PR to help you understand and configure settings before regular Pull Requests begin.

To activate Renovate, merge this Pull Request. To disable Renovate, simply close this Pull Request unmerged.

Detected Package Files

- `pom.xml` (maven)

Configuration Summary

Based on the default config's presets, Renovate will:

- Start dependency updates only once this onboarding PR is merged.
- Enable Renovate Dependency Dashboard creation.
- If Renovate detects semantic commits, it will use semantic commit type `fix` for dependencies and `chore` for all others.
- Ignore `node_modules`, `bower_components`, `vendor` and various test/tests directories.
- Autodetect whether to pin dependencies or maintain ranges.
- Rate limit PR creation to a maximum of two per hour.
- Limit to maximum 10 open PRs at any time.
- Group known monorepo packages together.
- Use curated list of recommended non-monorepo package groupings.
- A collection of workarounds for known problems with packages.



```
1 + {
2 +   "$schema": "https://docs.renovatebot.com/renovate-schema.json",
3 +   "extends": [
4 +     "config:base"
5 +   ]
6 + }
```

@MaritvanDijk77

Renovate configuration



- All repos or selected repos
- Config file is created for you
- Scheduling
- Max. number of PR's / concurrent branches
- Rule based auto merge
- More options & more fine-grained

<https://docs.renovatebot.com/configuration-options/>

@MaritvanDijk77

Renovate PR



Update jackson.version to v2.13.4 #64

[Open](#) renovate wants to merge 1 commit into `main` from `renovate/jackson.version` [Diff](#)

[Conversation 0](#) [Commits 1](#) [Checks 1](#) [Files changed 1](#)

renovate (bot) commented 12 days ago [Contributor](#) [...](#)

This PR contains the following updates:

Package	Change	Age	Adoption	Passing	Confidence
<code>com.fasterxml.jackson.core:jackson-databind (source)</code>	<code>2.9.7 -> 2.13.4</code>	160	15%	96%	neutral
<code>com.fasterxml.jackson.core:jackson-annotations (source)</code>	<code>2.9.7 -> 2.13.4</code>	160	11%	99%	high
<code>com.fasterxml.jackson.core:jackson-core</code>	<code>2.9.7 -> 2.13.4</code>	160	15%	97%	neutral

<https://docs.renovatebot.com/merge-confidence/>

@MaritvanDijk77

Renovate Dashboard: Project



Dependency Dashboard #68

Open

9 tasks

renovate · bot · opened this issue 21 hours ago · 0 comments



renovate · bot · commented 21 hours ago

Contributor

...

This issue lists Renovate updates and detected dependencies. Read the [Dependency Dashboard docs](#) to learn more.

Open

These updates have all been created already. Click a checkbox below to force a retry/rebase of any.

- [Update dependency com.thoughtworks.xstream:xstream to v1.4.19](#)
- [Update dependency junit:junit to v3.8.2](#)
- [Update spring core to v4.3.30.RELEASE \(org.springframework:spring-exn , org.springframework:spring-webmvc \)](#)
- [Update jackson:version to v2.13.4 \(com.fasterxml.jackson.core:jackson-databind , com.fasterxml.jackson.core:jackson-annotations , com.fasterxml.jackson.core:jackson-core \)](#)
- [Update dependency junit:junit to v4](#)
- [Update dependency org.hibernate:hibernate-validator to v8](#)
- [Update spring core to v5 \(major\) \(org.springframework:spring-exn , org.springframework:spring-webmvc \)](#)
- [Click on this checkbox to rebase all open PRs at once](#)

Detected dependencies

► maven

- [Check this box to trigger a request for Renovate to run again on this repository](#)

@MaritvanDijk77

Renovate Dashboard: Jobs



Renovate Dashboard Documentation Sign out

cucumber-json-converter
cucumber-json-schema
cucumber-junit-xml-formatter
cucumber-jvm
cucumber-jvm-groovy
cucumber-jvm-scala
cucumber-lua
cucumber-message-upload-service
cucumber-parent
cucumber-rails
cucumber-ruby
cucumber-ruby-core
cucumber-ruby-meta
cucumber-ruby-wire
cucumber-tcl-wire
cucumber.ml
demo-formatter
docs

cucumber/cucumber-jvm logs

Search

Job ID	Result	Date
991877684	dcne	16 minutes ago
991973171	dcne	4 hours ago
991905485	dcne	7 hours ago
991776931	dcne	11 hours ago
991631974	dcne	16 hours ago
991516227	dcne	28 hours ago
991448085	dcne	a day ago
991278531	dcne	a day ago
991201844	dcne	a day ago
991096790	dcne	a day ago
991977907	dcne	2 days ago
991886491	dcne	2 days ago
991554817	dcne	2 days ago
991326468	dcne	2 days ago
991118578	dcne	2 days ago
991883169	dcne	3 days ago
991653641	dcne	3 days ago
991388884	dcne	3 days ago

@MaritvanDijk77

Renovate: Supported platforms



- GitHub (.com and Enterprise Server)
- GitLab (.com and CE/EE)
- Bitbucket Cloud
- Bitbucket Server
- Azure DevOps
- AWS CodeCommit
- Gitea

<https://docs.renovatebot.com/#supported-platforms>

@MaritvanDijk77

Snyk Open Source



- Available via Snyk
- Features:
 - Security updates
 - Version updates
 - Test for new vulnerabilities (on PRs)
 - Test for vulnerabilities in source code
 - Dashboards

<https://snyk.io/>

@MaritvanDijk77

Snyk enable



snyk Products Resources Company Pricing Log In Book a live demo Sign up

Developer loved, Security trusted.

Find and automatically fix vulnerabilities in your code, open source dependencies, containers, and IaC – powered by Snyk's industry-leading security intelligence and DeepCode AI.

[Start free](#) [Book a live demo →](#)

<https://snyk.io/>

@MaritvanDijk77



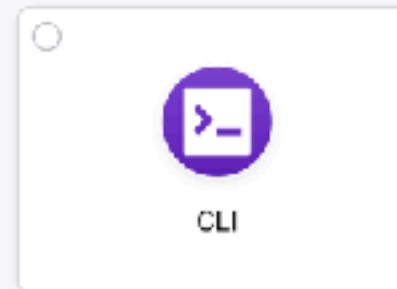
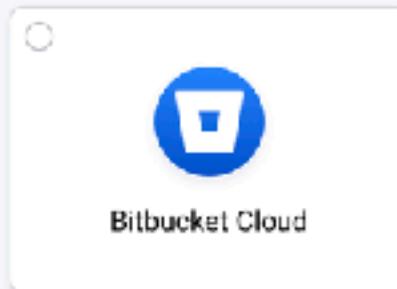
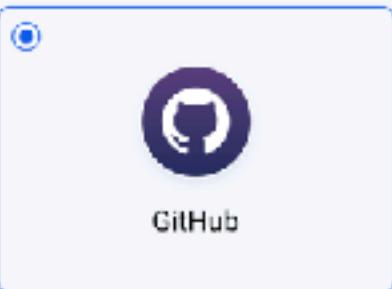
Snyk enable

Where is the code you want to scan?

Scan your projects for security issues

1 Choose integration method

Connect Snyk to your code and run scans directly in your workflow



Next step

Not what you're looking for?

[View all integrations](#) OR [Learn more about integrations](#)

2 Set access permissions

3 Configure automation settings & authenticate

@MaritvanDijk77



Snyk enable

Where is the code you want to scan?

Scan your projects for security issues

✓ Choose integration method

2 Set access permissions



Private and public repositories

Grant Snyk access to all repository types under your Github account whether private or public.



Public repositories only

Grant Snyk access to repositories marked public under your Github account.

Once authenticated, Snyk:

- ✓ Scans the directory trees of selected repos and automatically represents them as projects
- ✓ Generates security reports that enable you to explore issues in your repositories and assist you with fixing them
- ✓ Continuously checks imported projects for vulnerabilities. When new vulnerabilities are found, you'll be notified

Next step

Previous

3

Configure automation settings & authenticate

@MaritvanDijk77



Snyk enable

- ✓ Choose integration method
- ✓ Set access permissions
- 3 Configure automation settings & authenticate

Enabled features:

Pull Request Checks

Test your pull requests for new issues and vulnerabilities

New Fix Pull Requests

Automatically create pull requests for newly discovered open source issues and vulnerabilities

Dependency Upgrade Pull Requests

Keep your packages up to date with automatic dependency upgrade pull requests

Snyk Code

Analyze your source code for issues and vulnerabilities ⓘ

[Authenticate GitHub](#)

[Previous](#)

@MaritvanDijk77

Snyk enable



Authorize Snyk



Snyk by Snyk

wants to access your mlvandijk account



Organizations and teams

Read-only access



Repositories

Public and private



Personal user data

Email addresses (read-only)



@MaritvanDijk77

Snyk PR



[Snyk] Security upgrade com.fasterxml.jackson.core:jackson-databind from 2.9.7 to 2.9.10.7 #47

Edit < Code

Open snyk-bot wants to merge 1 commit into main from snyk-fix-6545eb40e5d321178cd9bca857119a65

Conversation 0 Commits 1 Checks 0 Files changed 1

+1 -1



snyk-bot commented on 19 Jan 2021

First-time contributor

Snyk has created this PR to fix one or more vulnerable packages in the 'maven' dependencies of this project.

Changes included in this PR

- + Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Upgrade	Breaking Change
H	681/1000 Why? Recently disclosed, Has a fix available, CVSS 8.1	Deserialization of Untrusted Data SNYK-JAVA-COMFASTERXMLJACKSONCORE-1061931	com.fasterxml.jackson.core:jackson-databind: 2.9.7 -> 2.9.10.7	No

Reviewers

No reviews

Still in progress? Convert to draft.

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

@MaritvanDijk77



Snyk PR

[Snyk] Fix for 5 vulnerabilities #49

[Open](#) mlvandijk wants to merge 1 commit into [main](#) from [snyk-fix-894f735a21477e79bcea4d6278b3dtba](#) [Diff](#)

Conversation 0 · Commits 1 · Checks 0 · Files changed 1



mlvandijk commented on 21 Feb 2021

Owner ...

Snyk has created this PR to fix one or more vulnerable packages in the 'maven' dependencies of this project.

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Upgrade	Breaking Change	Exploit Maturity
H	644/1000 Why? Has a fix available, CVSS 8.6	Improper Input Validation SNYK-JAVA-ORGSPRINGFRAMEWORK-1009832	org.springframework:spring-webmvc 4.3.5.RELEASE -> 4.3.29.RELEASE	No	No Known Exploit
M	609/1000 Why? Has a fix available, CVSS 5.9	Information Exposure SNYK-JAVA-ORGSPRINGFRAMEWORK-31689	org.springframework:spring-webmvc 4.3.5.RELEASE -> 4.3.29.RELEASE	No	No Known Exploit

@MaritvanDijk77

Snyk PR Check



 **All checks have passed** [Hide all checks](#)

 **1 successful check**

 ✓	security/snyk (mlvandijk) — 1 security test has passed	Details
---	---	-------------------------

@MaritvanDijk77

Snyk dashboard



snyk

mlvandijk > Dashboard

Add projects

ORGANIZATION
mlvandijk

Dashboard

Projects

Integrations

Members

Settings

Help

Marit van Dijk

Pending tasks

Snyk tracks and flags Pull Requests (PRs) in the top most vulnerable projects

PROJECT	FIXABLE ISSUES	ACTIONS
mlvandijk/kotlin-bootique	19 C 50 H 21 M 3 L	Fix vulnerabilities
mlvandijk/rugbymatch	19 C 50 H 16 M 3 L	Fix vulnerabilities

Vulnerable projects

Projects with vulnerabilities detected

PROJECT	TESTED	ISSUES	ACTIONS
mlvandijk/kotlin-bootique:pom.xml	Mar 2, 2021	0 C 69 H 21 M 3 L	Fix vulnerabilities
mlvandijk/rugbymatch:pom.xml	Mar 2, 2021	0 C 69 H 16 M 3 L	Fix vulnerabilities
mlvandijk/springbootproject:pom.xml	Mar 2, 2021	0 C 67 H 15 M 3 L	Fix vulnerabilities
mlvandijk/tul-restnonrest:pom.xml	Mar 2, 2021	0 C 65 H 9 M 4 L	Fix vulnerabilities

Issues summary

SECURITY ISSUES

Critical

0

High

1015

Medium

329

Low

74

[Learn about reports](#)

@MaritvanDijk77

Snyk Open Source Configuration



- Frequency (daily, weekly, never)
- Enable/disable: New and/or known vulnerabilities
- Enable/disable PR's for single project

<https://docs.snyk.io/products/snyk-open-source/open-source-basics>

@MaritvanDijk77

Snyk Open Source: Supported Platforms



- GitHub
- GitHub Enterprise
- GitHub Read-only projects
- Bitbucket Cloud Personal Access Token (Legacy)
- Bitbucket Cloud App
- Bitbucket Data Center/Server
- GitLab
- Azure Repos

<https://docs.snyk.io/integrations/git-repository-scm-integrations>

@MaritvanDijk77

Bots

 Dependabot

 Renovate

 Snyk Open Source



@MaritvanDijk77

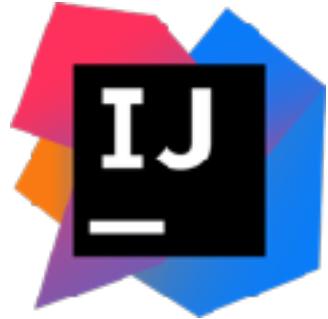
Bots: Pros & Cons

- + Relatively easy to install
- + Automatic PR's
- Can create "noise"
- Manage PRs (merge & deploy)
- No code changes (if needed)

Migration tools

@MaritvanDijk77

IntelliJ IDEA



- Refactor > Migrate Packages and Classes

A screenshot of the IntelliJ IDEA interface. The window title is "IntelliJ IDEA". The menu bar includes File, Edit, View, Navigate, Code, Refactor, Build, Run, Tools, Git, Window, Help. The "Refactor" menu is open, showing various options like Refactor This..., Rename..., Rename File..., Change Signature..., Extract/Inline, Inline to Anonymous Class, Find and Replace Code Duplicates..., Move Classes..., Copy Class..., Delete Class..., Pull Members Up..., Push Members Down..., Type Migration..., Make Static..., Convert to Instance Method..., Use Interface Where Possible..., Replace Inheritance with Delegation..., Encapsulate Fields..., Migrate Packages and Classes..., Convert Raw Types to Generics..., Invert Boolean..., Introduce Variable..., Migrate to Android..., Migrate to Non-Testable & Classes..., and Create New Migration... (disabled). The "Migrate Packages and Classes..." option is highlighted with a red box. The code editor shows Java test code with annotations like @BeforeAll, @Test, and @Disabled. The status bar at the bottom right shows "332 1P 1M 1S 8 spaces 10".

<https://www.jetbrains.com/help/idea/migrate.html>

@MaritvanDijk77

IntelliJ IDEA



- Refactor > Migrate Packages and Classes >
 - Java EE to Jakarta EE
 - JUnit (4.x -> 5.0)
 - JavaFX (8 -> 9)

A screenshot of the IntelliJ IDEA interface showing the 'Refactor' menu open. The 'Migrate Packages and Classes' option is highlighted with a blue bar. A dropdown menu is displayed with several options:

- Migrate Packages and Classes (highlighted)
- >
- Java EE to Jakarta EE
- JUnit (4.x -> 5.0)
- JavaFX (8 -> 9)
- Create New Migration...

The background shows other menu items like 'Convert Raw Types to Generics...', 'Invert Boolean...', and 'Internationalize...'.

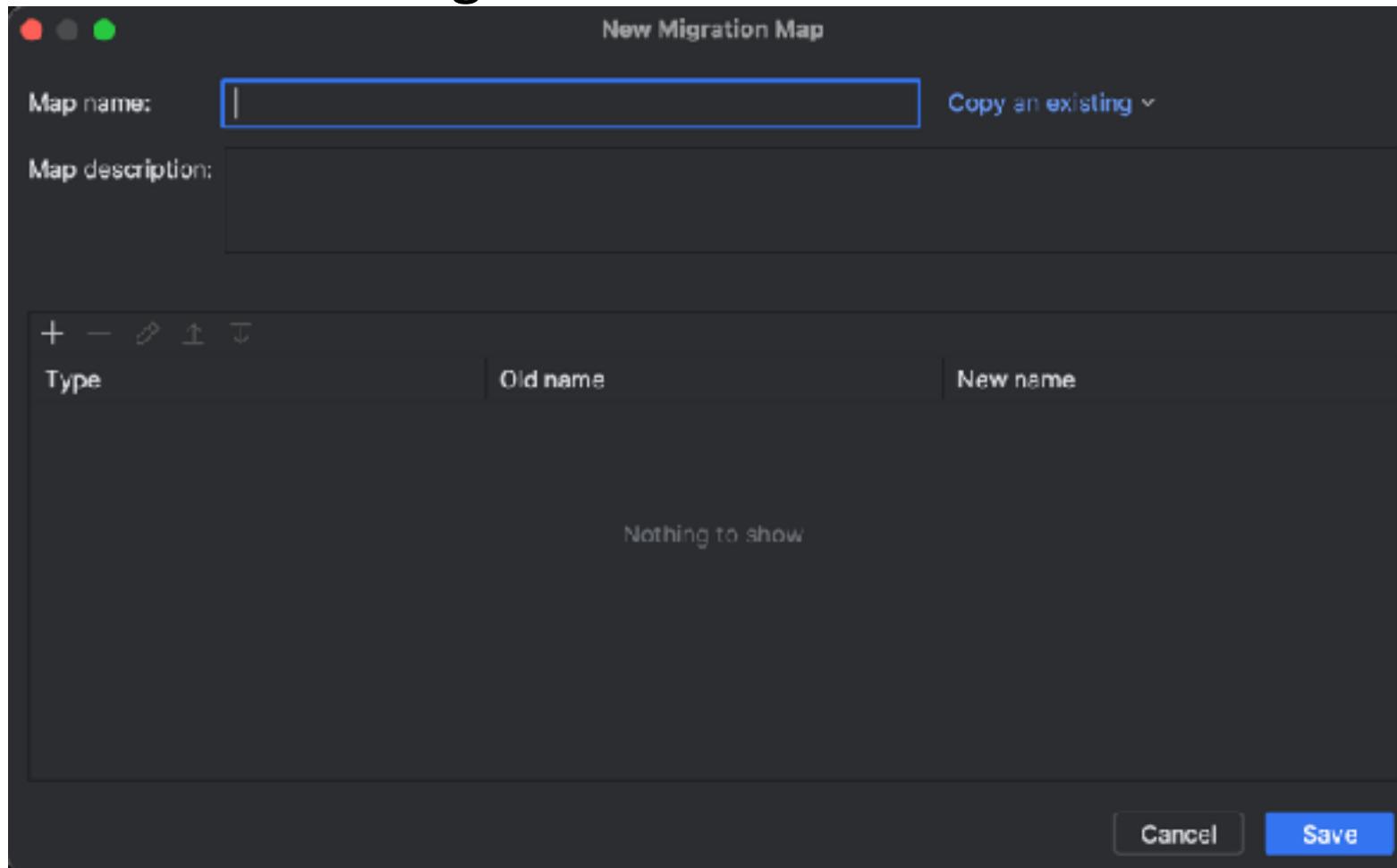
<https://www.jetbrains.com/help/idea/migrate.html>

@MaritvanDijk77

IntelliJ IDEA



- Create New Migration



@MaritvanDijk77

IntelliJ IDEA



- Create New Migration

New Migration Map

Map name: JUnit (4.x -> 5.0)

Map description: For transferring the JUnit 4 test annotations to the new jupiter ones, may result in red code! Assertions won't be migrated. Please see the 'Java | JUnit Issues | JUnit 4 test can be JUnit 5' Inspection to migrate only tests which can be converted fully automatically.

Type	Old name	New name
Class	org.junit.Before	org.junit.jupiter.api.BeforeEach
Class	org.junit.BeforeClass	org.junit.jupiter.api.BeforeAll
Class	org.junit.After	org.junit.jupiter.api.AfterEach
Class	org.junit.AfterClass	org.junit.jupiter.api.AfterAll
Class	org.junit.Test	org.junit.jupiter.api.Test
Class	org.junit.Ignore	org.junit.jupiter.api.Disabled

Cancel Save

@MaritvanDijk77

IntelliJ IDEA

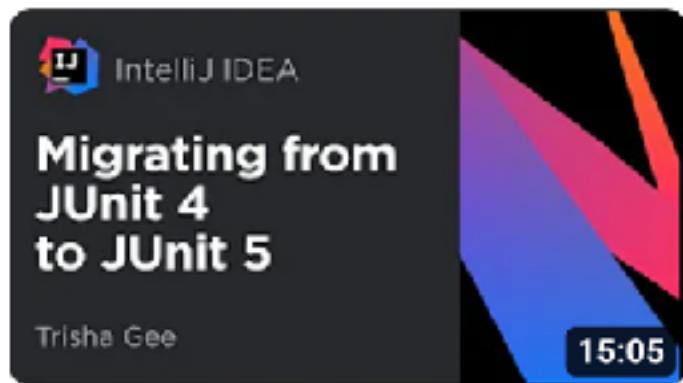


Migrating from javax to jakarta namespace

IntelliJ IDEA by JetBrains • 14K views • 11 months ago

In this video, we'll look at how to migrate an application from using the javax namespace to the jakarta namespace. This change is expected to impact a lot of enterprise Java developers, especially...

CC



IntelliJ IDEA. Migrating from JUnit 4 to JUnit 5

IntelliJ IDEA by JetBrains • 18K views • 2 years ago

JUnit has been around for a long time, and many applications will have a large number of JUnit tests written using JUnit 4. JUnit 5 was released in 2017, and provides a lot of features that...

CC

<https://www.youtube.com/@intellijidea>

@MaritvanDijk77

Error Prone

- **Static analysis tool** for Java to **catch common programming mistakes** at compile-time.
- Maven, Gradle, etc.
- IntelliJ IDEA / Eclipse plugin, Command line
- Bug patterns
- Report or fix
- Custom checks
- Includes **Refaster**: refactor code using before-and-after templates

Error Prone

Error Prone



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

@MaritvanDijk77

Error Prone Support



Bug Patterns

Refaster Rules

Error Prone Support

Error Prone Support is a [Picnic](#)-opinionated extension of Google's [Error Prone](#). It aims to improve code quality, focussing on maintainability, consistency and avoidance of common pitfalls.

<https://error-prone.picnic.tech/>

@MaritvanDijk77



OpenRewrite

- **Source code refactoring** for framework/API migrations, vulnerability patches, and static code analysis fixes
- Java, Kotlin & Groovy support
- Run with Maven or Gradle
- Run without a build tool
- Early support for Python, Typescript, ...

OpenRewrite



- Existing recipes
 - Upgrade versions
 - Migrate libraries

Popular recipe guides

Here are the articles in this section:

[Common static analysis issue remediation](#)

[Automatically fix Checkstyle violations](#)

[Migrate to Java 17](#)

[Migrate to JUnit 5 from JUnit 4](#)

[Migrate to Spring Boot 3 from Spring Boot 2](#)

[Migrate to Spring Boot 2 from Spring Boot 1](#)

[Migrate to Quarkus 2 from Quarkus 1](#)

[Migrate to Micronaut 4 from Micronaut 3](#)

[Migrate to Micronaut 3 from Micronaut 2](#)

[Migrate to SLF4J from Log4J](#)

[Use SLF4J parameterized logging](#)

[Refactoring with declarative YAML recipes](#)

[Automating Maven dependency management](#)

[Migrate Hamcrest to AssertJ](#)

OpenRewrite

- Existing recipes
 - Find by topic

Recipe catalog

Here are the articles in this section:

Kotlin	Python
Analys	CircleCI
Cloud suitability analyzer	Concourse
Cucumber	Github Actions
Hibernate	Java
Jenkins	Kubernetes
XML	Micrometer
Okio	OkHttp
Quarkus	Recommendations
Gradle	Maven
SQL	Static analysis and remediation



OpenRewrite



- Existing recipes
- Can author your own recipes

<https://docs.openrewrite.org/>

@MaritvanDijk77

OpenRewrite

Rewrite

Moderne

Search recipes like java + K P

Spring Patch | ⚙ | ⚙ | ⚙

RECIPIES

- Marketplace
- Build
- Deploy

ORGANIZATIONS

- Repositories

RESULTS

- Recent recipes
- Recent commits

ADMIN

- Agents
- Audit logs
- Workers

https://app.moderne.io/recipes/org.openrewrite.java.migrate.lang.UseTextBlocks?defaults=W3sibmFtZSI6ImNvbnZlc...
TIM TE BEEK
MAJOR MIGRATIONS MADE EASY

42:52

<https://www.youtube.com/watch?v=jOFFCAleUI8>

@MaritvanDijk77

Conclusion

- (Re)evaluate dependencies carefully
- Automate checks & updates
- Stay safe!

Slides & More

<https://maritvandijk.com/presentations/keep-your-dependencies-in-check/>



@MaritvanDijk77

goto;

Don't forget to
rate this session
in the **GOTO Guide app**