THE TIDELIFT MAINTAINER ADVANTAGE

Eliminating the risk of RCE vulnerabilities in jackson-databind

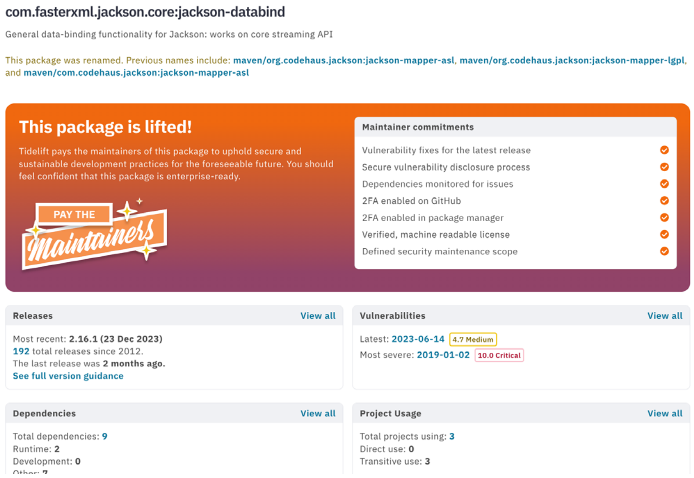
jackson-databind is an extremely popular general-purpose java data-binding package. It's used in a wide variety of applications to read content encoded in JSON and other popular formats.

jackson-databind is used by many of Tidelift's customers. Several of these customers have shared how important jackson-databind is to their applications, but also expressed concerns that it was being impacted by a large number of remote code execution (RCE) vulnerabilities. This was adding to increased security risk in impacted applications, and at least one customer was already planning to re-architect jackson-databind out of the infrastructure unless this risk could be decreased.

Tatu Saloranta, sometimes known as "Dr. Jackson," is the maintainer of jackson-databind and the creator of the Jackson data processor. Tatu is also the author of many other OSS libraries for Java, from ClassMate to Woodstox. Most importantly, Tatu is an independent open source maintainer who works on jackson-databind mostly outside of work on his own time..

Tatu is also a Tidelift partnered maintainer, who is paid by Tidelift to implement enterprise class secure software development practices, and to ensure jackson-databind continues to follow these practices into the future. Thanks to the income made possible by Tidelift customers (Tidelift pays maintainers based on factors like customer usage and package criticality), Tatu has been able to document that jackson-databind follows important secure development practices, including providing vulnerability fixes for the latest release, monitoring dependencies for issues, having 2FA enabled, having a secure vulnerability disclosure process, and more.

Even better, when it comes to the remote code execution vulnerabilities that were of concern to Tidelift's customers using jackson-databind, Tatu was able to use the income from Tidelift and its customers to devote the time and resources to completely re-architecting jackson-databind to eliminate the risk of RCE vulnerabilities once and for all.



com.fasterxml.jackson.core:jackson-databind

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

This package was renamed. Previous names include: maven/org.codehaus.jackson:jackson-mapper-asl, maven/org.codehaus.jackson:jackson-mapper-lgpl, and maven/com.codehaus.jackson:jackson-mapper-asl

This package is lifted!

Tidelift pays the maintainers of this package to uphold secure and sustainable development practices for the foreseeable future. You should feel confident that this package is enterprise-ready.

Maintainer commitments

- Vulnerability fixes for the latest release ✓
- Secure vulnerability disclosure process ✓
- Dependencies monitored for issues ✓
- 2FA enabled on GitHub ✓
- 2FA enabled in package manager ✓
- Verified, machine readable license ✓
- Defined security maintenance scope ✓

Releases — View all

Most recent: **2.16.1 (23 Dec 2023)**
192 total releases since 2012.
The last release was **2 months ago.**
See full version guidance

Vulnerabilities — View all

Latest: 2023-06-14 4.7 Medium
Most severe: 2019-01-02 10.0 Critical

Dependencies — View all

Total dependencies: 9
Runtime: **2**
Development: **0**
Other: 7

Project Usage — View all

Total projects using: 3
Direct use: **0**
Transitive use: **3**

Here is the jackson-databind package page inside of the Tidelift application, showing the secure development practices the project is following, and also including additional useful information about releases, vulnerabilities, dependencies, and where it is being used within an example organization.

In fact, one customer reported that while jackson-databind had previously been on a list of packages to re-architect out of its applications because it had received an internal risk calculation score that was higher than acceptable, the risk calculation score had been reduced substantially and it was no longer on the list of packages to be removed.

Now, Tidelift customers can use jackson-databind—and other packages that rely on it—with confidence, knowing that Tatu has made the commitment to ensure the package follows enterprise secure software development practices. What's more, Tidelift customers directly played a role in funding work on jackson-databind so that Tatu can make investments in ensuring it stays resilient and healthy into the future.