

Closed Opened 1 week ago by  muffinx

jackson-databind Remote Command Execution

Dear E-Voting PIT Team

We saw that you have a lot of dependencies and of course these aren't scope of this PIT.

Nevertheless, this one shook us really, since on this one, there are so many vulnerabilities.

Please take this one really serious.

No normally jackson 2.9.5 is used, which is alright:

```
evoting-solution-master/source-code/online-voting-secure-data-manager/pom.xml:
<jackson.version>2.9.5</jackson.version>
evoting-solution-master/source-code/online-voting-channel/pom.xml:           <jackson.version>2.9.5</jackson.version>
```

But in the online-voting-mixing 2.8.9 is used:

```
evoting-solution-master/source-code/online-voting-mixing/pom.xml:           <jackson.version>2.8.9</jackson.version>
```

Now, 2.8.9 has 10 CVE's registered!

https://www.cvedetails.com/vulnerability-list/vendor_id-15866/product_id-42991/version_id-238178/Fasterxml-Jackson-databind-2.8.9.html

These vulnerabilities can be used to pretty simply pwn the mixing backend.

Here a critical one:

```
CVE-2018-7489
FasterXML jackson-databind before 2.7.9.3, 2.8.x before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code ex
```


And CVE-2017-7525 which is mentioned in CVE-2018-7489 is very easy to exploit:

<https://adamcaudill.com/2017/10/04/exploiting-jackson-rce-cve-2017-7525/>

Thank you very much for reading our report.

Best Regards

Anthony Schneider aka. muffinx Jannis Kirschner aka. xorkiwi

 Swisspost @swisspost added In Progress topic: general labels 1 week ago



Swisspost @swisspost · 1 week ago

Maintainer

Hello Anthony,

Thank you for your input. We will verify this and get back to you.

Kind regards






Swisspost @swisspost · 1 week ago

Maintainer

Hello Anthony,

The mixing module is used in the online-voting-channel and in the secure data manager. In both projects, the version is superseded by the versions defined in the respective projects. Online-voting-channel and the secure data manager use Jackson version 2.9.5. For the sake of clarity, we take note to update the dependencies in the mixing pom, but these transitive dependencies do not reach the compiled binaries.

Kind regards

-  [Swisspost @swisspost](#) closed [1 week ago](#)
-  [Swisspost @swisspost](#) removed [In Progress](#) label [1 day ago](#)
-  [Swisspost @swisspost](#) made the issue visible to everyone [1 day ago](#)