



## RxCheck SRS 3.1 Build#70 Patch Release

April 15, 2024

*This patch release is an update to specific third-party libraries. The update specifically addresses identified security issues in Apache Tomcat and Spring Framework, ensuring enhanced protection for your system. This proactive measure demonstrates RxCheck's commitment to continuously fortifying the platform against potential vulnerabilities. Ensuring the security and integrity of your data remains RxCheck's top priority.*

The following libraries are updated:

- Apache Tomcat to v9.0.86
- Spring Framework to v5.3.33

**The following vulnerabilities are addressed in this patch:**

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22243>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22259>

**Patch download location:**

[http://builds.rxcheck.org/SRS/v3.1/public\\_final/patches/](http://builds.rxcheck.org/SRS/v3.1/public_final/patches/)

**Assumptions:**

This patch assumes you already have an SRS v3.1 running on your servers. No development will be required by states or vendors.

**Steps to apply the patch:**

1. Download new **rxoutbound.war** and **rxinbound.war** files from the patch location.
2. Shutdown current RxCheck SRS v3.1 process.
3. Take a backup of all the files and folders under the **webapps** folder of the SRS installation.
4. Delete all files and folders under **webapps** folder of the SRS installation.
5. Copy the new **rxoutbound.war** file to the **webapps** folder.
6. Copy the new **rxinbound.war** to the **webapps** folder.
7. Start the RxCheck SRS v3.1 process.

**IT/Vendor Questions:**

If your IT/vendor personnel would like to discuss this patch release or have technical questions, please have them email Ron Larsen at IJIS at [ron.larsen@ijis.org](mailto:ron.larsen@ijis.org).

Field Code Changed