

Field Security Plugin Security Advisory 2019-06-26

Issue 1

Under some circumstances a user with access rights limited according to the field security scheme may be able to access a hidden field and/or modify a read-only field via the REST API.

This issue affects only security features provided by Fields Security Plugin and does not affect any core JIRA features.

This vulnerability is rated as **Critical** according to [Atlassian's Severity Levels for Security Issues](#).

This issue affects all JFS versions for JIRA 7.0-8.2 starting from JFS 1.4.31_70 and up and is fixed in JFS 1.4.53 for JIRA 7.2-8.2.

How to fix

JIRA 7.2 and later

Upgrade to JFS 1.4.53. There is no need to re-apply the JFS patch.

1. [Ensure support & maintenance is active](#) for your license.
2. Navigate to [Downloads page](#)
3. Download JFS 1.4.53 addon JAR file according to your JIRA version
4. Upgrade the addon using JIRA Universal Plugin Manager ("Manage Add-ons")
5. Restart your JIRA instance immediately (Note: this is mandatory!)
6. There is no need to re-apply the JFS patch

Please contact support@quisapps.com in case of any questions.

JIRA 7.1 and prior

If you are still using JIRA 7.0 or 7.1, please contact support@quisapps.com.

Consider upgrading to more recent versions of JIRA and JFS.