

Field Security Plugin Security Advisory 2014-04-15

Issue 1

A user with restricted access can view secured field values via 'Jump to Field' JIRA feature.

This issue affects all JFS versions up to and including 1.4.18 for JIRA 6.0, 6.1, 6.2 and is fixed in JFS 1.4.19 for JIRA 6.0 and 6.1 and in JFS 1.4.20 for JIRA 6.2. This issue does not affect JFS for JIRA 5.2 and prior.

Issue 2

A user with restricted access can view secured field values or perform Assign Issue operation via JIRA Mobile plugin.

This issue affects all JFS versions up to and including 1.4.19 for JIRA 6.0, 1.4.19 for JIRA 6.1 and 1.4.20 for JIRA 6.2 and is fixed in JFS 1.4.21 for JIRA 6.0, 6.1, 6.2. This issue does not affect JFS for JIRA 5.2 and prior.

Issue 3

Cross-site scripting (XSS) vulnerabilities have been identified and fixed. XSS vulnerabilities allow an attacker to embed their own JavaScript into a JIRA page.

This issue affects all JFS versions for all JIRA versions up to and including 1.4.21 and is fixed in JFS 1.4.22.

How to fix

JIRA 5.2 and later

Upgrade to JFS 1.4.22.

1. Navigate to [Downloads page](#)
2. Download JFS 1.4.22 plugin JAR file according to your JIRA version
3. Upgrade the plugin using JIRA Universal Plugin Manager
4. Restart your JIRA instance (Note: this is mandatory!)
5. There is no need to re-apply the JFS patch

JIRA 5.1 and prior

Please note that Issue 3 only affects JFS for JIRA 5.1 and prior.

Updated versions

- JFS for JIRA 5.1: 18/Apr/14

If you use JIRA 5.0 or prior please contact support@quisapps.com to receive the updated JFS build for your JIRA version.