

SonarQube/SonarCloud issue report in Jira Issue Tab

Since 2.12 version you can view a SonarQube/SonarCloud issue report from Jira Issue Tab.

In this report, developers can directly access the line of code where the issue is located in SonarQube / SonarCloud.

Issue Report for SonarQube/SonarCloud Issues

The screenshot shows the SonarQube interface for the rule 'Cognitive Complexity of methods should not be too high'. The rule is marked as 'Confirmed' and has a 'Severity' of 'Error'. The table below shows 5 issues, all of which are 'Open' and have a 'Type' of 'Bug'.

Severity	Issue	Confirmed	Required	Blocked	Closed	Type	Line	Status
Error	src_..._backlogItemsBatchUpdateSQLLine Refactor this method to reduce its Cognitive Complexity from 43 to the 10 allowed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bug	1459	Open
Error	src_..._backlogItemsBatchUpdateSQLLine Refactor this method to reduce its Cognitive Complexity from 10 to the 10 allowed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bug	1789	Open
Error	src_..._backlogItemsBatchUpdateSQLLine Refactor this method to reduce its Cognitive Complexity from 21 to the 10 allowed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bug	1862	Open
Error	src_..._backlogItemsBatchUpdateSQLLine Refactor this method to reduce its Cognitive Complexity from 33 to the 10 allowed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bug	1508	Open
Error	src_..._backlogItemsBatchUpdateSQLLine Refactor this method to reduce its Cognitive Complexity from 10 to the 10 allowed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bug	1345	Open

Issue Report for SonarQube/SonarCloud Security Hotspot

Using Components with Known Vulnerabilities

Details

Type: **Historia**

Affects Version(s): **None**

Status: **Unresolved** (View Workflow)

Resolution: **None**

Fix Version(s): **None**

Description

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or service disruption. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

- **CVE-2013-0236** **LOW**
- **DNSMAP Test To 2013-AD Using Components with Known Vulnerabilities**(https://www.mend.io/advisories.php?Test_To_2013-AD-Using_Components_with_Known_Vulnerabilities)
- **[Common Weakness Enumeration CVE-937]**(<https://nvd.nist.gov/vuln/detail/CWE-937>)
- **[Dependency Check]**(https://www.mend.io/advisory/CVNDOSMAP_Dependency_Check)

Go to check your Security Histograms to SonarQube project: [SonarQube Connector for Jira](#)

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity Source **SonarQube**

Priority	Security Histogram	42	2 Reviewed	Type	Line	Status	Resolution
LOW	CVE-2019-14644	Flascore: spring-data-commons-1.8.1.BUILD-SNAPSHOT Highest CVSS Score: 9.8 Amount of CVE's: 1 References: CVE-2018-1273 (8.8)	1	Reviewed	FIXED		
LOW	CVE-2019-14644	Flascore: Spring-core>=3.0.2.1-jar Highest CVSS Score: 8.5 Amount of CVE's: 3 References: CVE-2018-20233 (8.5) CVE-2018-8229 (8.5) CVE-2019-14644 (8.2)	1	Reviewed	SAFE		
LOW	CVE-2019-14644	Flascore: lang-js-1.2.8-jar Highest CVSS Score: 9.8 Amount of CVE's: 2 References: CVE-2019-17571 (8.8) CVE-2020-0488 (8.7)	1	To Review			
LOW	CVE-2019-14644	Flascore: langjs-testcases-origins-2.2-sources.jar Highest CVSS Score: 3.7 Amount of CVE's: 1 References: CVE-2020-0488 (3.7)	1	To Review			
LOW	CVE-2019-14644	Flascore: Spring-security-5.3.0-alibaba3-jar Highest CVSS Score: 8.8 Amount of CVE's: 7 References: CVE-2019-16010 (8.8) CVE-2019-20087 (8.8) CVE-2020-08213 (7.8) CVE-2017-16024 (8.5) CVE-2018-4220 (8.5) CVE-2017-16014 (8.5) CVE-2019-16001 (8.5)	1	To Review			