SonarQube 9.4

SonarQube 9.4 - GCP Terraform

April 2022

Edited by ALM-Toolbox (https://almtoolbox.com/sonarqube)

More rules and faster analysis

SonarQube 9.4 offers an exciting mix of new features and improvements, including lots of new rules across languages; significant speed improvements for Java analysis; improved and expanded Java taint analysis; better C and C++ analysis accuracy; additional security reporting and an updated Portfolio PDF format!

Terraform for GCP, plus improved Security Hotspots review

Helping you secure your cloud-native apps remains a top priority, and with SonarQube 9.4 we've added Terraform rules specifically for Google Cloud Platform and Azure Cloud. For GCP a total of 17 new rules cover permissions, encryption at rest and in transit, and traceability / logging. We've also expanded Terraform for Azure Cloud with three new traceability / logging Security Hotspot rules.

And because cloud-related Security Hotspots can be a little more complicated than those in other code, we've improved the overall Security Hotspot experience. First, we've added the display of secondary locations - those locations that contribute to the problem. Seeing those additional locations will help you understand the problem and how to address it. And because infrastructure-related Security Hotspots may not be fixable at the drop of a hat, we've added the ability to "acknowledge" them as needing a fix during review. Acknowledging a Security Hotspot marks it as reviewed. And when it's time, you'll be able to easily re-find it using the Acknowledged filter.

Java analysis 30% faster on average

You already know Java analysis offers valuable rules with high precision. Now it's moving into the realm of high performance with analysis speed improvements of up

to 67%. One beta tester said analyzing their 1 million LoC project dropped from 38 minutes to 18. Larger projects will see a greater benefit, but our tests across projects show an average 30% improvement in the speed of the Java sensor.

Many times analysis faces a speed / precision tradeoff, but these gains come from more efficient file handling. Instead of processing them one by one, we're now able to handle related files in batches. That means faster analysis with no loss of precision.
And for commercial editions, we've further amped-up analysis speed on PRs - another 8-25%! - by limiting what we analyze. Starting with 9.4, only the changed files in a PR are fully analyzed. For unchanged files, we'll run only the rules that require structure / cross-file information. That is, we'll re-run the rules that might be impacted by changes in other files. (You'll find a full list of rules in the docs.) Most issues in unchanged files are suppressed in PR analysis, but issues with secondary locations on changed lines do show up. So you get the best of both worlds: faster PR analysis with issues created in old code by those new changes.

If you're coding in another language, don't be jealous. We anticipate rolling these changes out to other languages later this year.

OWASP Top 10 2021 support

The OWASP Foundation released an updated Top 10 list late last year that shuffled some existing categories around and added three new ones. With SonarQube 9.4, we've added support for that updated list side-by-side with OWASP Top 10 2017. You'll find that the relevant existing rules have been updated to reference the new list. And on the rules and issues pages, you'll be able to filter issues by the new categories.

In Enterprise Edition, we've added a report for the 2021 categories that you'll find both in the UI and in the Security Report PDF.

Taint analysis adds detection of less obvious Java vulnerabilities DE EE DCE

Java taint analysis has expanded to better cover your code with more rules and a better understanding of dependencies to detect additional true positives that were previously hidden.

This starts with two new injection-related rules for reflection and NoSQL and an expansion of the JSON and XML injection rules to include file writes. Next is a new rule to detect when thread suspension is vulnerable to DoS attacks. And finally, in all editions there are four new rules for additional types of insecure XML processing: inclusion of arbitrary files, loading of external schemas, signature validation, and detection of XML bombs.

These new rules - plus all the existing taint analysis rules - will benefit from work we've done to follow dataflow inside ten popular Java libraries to find more injection flaws than before: Apache HttpClient, Spring Boot Starter Web, Apache Log4j Core,

H2 Database Engine, MySQL Connector/J, HttpClient, Xerces2 J, MongoDB Driver, Dom4j, Retrofit.

Smoother, smarter SonarLint experience

SonarLint users will benefit from automatic syncs of Quality Profile changes. Rather than having to manually pull changes, this will happen automatically in the background. So you're always up to date in the IDE with the rules that will be applied during SonarQube analysis. This is already available in JetBrains IDEs, with Eclipse and VS Code expected very soon. And all three IDEs now also get quick fixes for JavaScript and TypeScript, both in standalone mode and when connected to SonarQube 9.4.

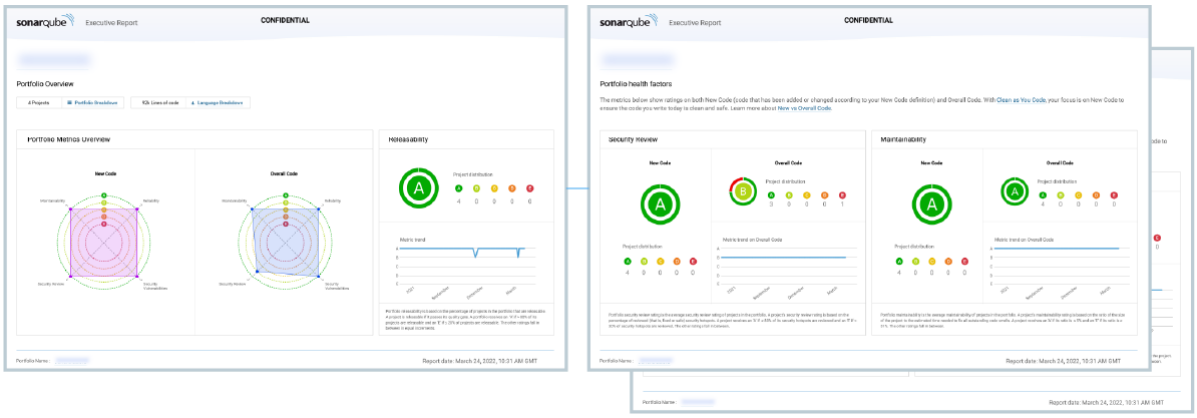
Improved precision, compiler support for C++ and C DE EE DCE

An improved handling of header files means fewer false negatives. With SonarQube 9.4, we make the distinction between system and user headers, to analyze the latter appropriately. This means fewer false negatives for most rules. And especially for advanced bug rules, such as S2259, which detects null pointer dereferences, there are fewer false negatives.

We've also improved analysis configuration across most popular compilers. This includes compile flags for ARMCC, Diab, Texas Instruments, and IAR; as well as compile flags and predefined value settings for MSVC; and compile flags and commands for CLang / GCC.

Portfolio PDF updated for Clean as You Code EE DCE

In SonarQube 9.3, the Clean as You Code method arrived in Enterprise Edition Portfolios. Now it's reflected throughout the Portfolio PDF as well. So the communication about New Code is consistent across the board: from project to Portfolio to PDF.



Language Updates

- Python:
  - 8 new rules for better regex writing (for a total of 21)
  - 8 new Code Smell rules
  - 1 new Bug rule
- TypeScript: Parse TypeScript 4.5 constructs
- Java: Parse Java 18