

Container Security v1.x

Release Notes for Bamboo Plugin

Version 1.4.3.0

December 4, 2018

Here's what's new in the Bamboo Plugin for Container Security!

[Build failure by Software](#)

[Criteria evaluation summary in reports](#)

Build failure by Software

Along with Vulnerabilities, QIDs, and CVEs, you can now fail the docker build if specific software is found in the image. In the build fail conditions in global/local config, you can specify a comma separated list of software names with or without version numbers. If this software is found, the build fails.

Provide software names in the format:

Name only:
rpm-libs


Name + version:
Rpm-libs=4.8.0-55.el6

Build Failure Conditions

You can fail the docker build under certain conditions. The build will fail when ANY of the selected conditions are met.

- Fail build if severe vulnerabilities found
Enter a threshold number exceeding which the build should fail; eg. Severity 3 count is set as 2; then if vulnerabilities with Severity 3 found are more than 2, build will fail.
- Fail build if any of these QIDs found
- Fail build if any of these CVEs found
- Fail build if any of these Softwares found
A comma separated list of Softwares to be evaluated for build failure. It can be simple comma separated list of software names with or without specific version. Software names with version should be provided in format - Softwarename={version} eg. rpm-libs=4.8.0-55.el6

Softwares*



Apply above fail conditions to potential vulnerabilities as well

Criteria evaluation summary in reports

The Qualys report for Bamboo will now show the criteria against which the image got evaluated for build failure.

The Criteria Evaluation table shows whether the criteria is configured or not, and the respective fail/pass result.

The screenshot shows a Qualys image scan report for a failed job. The main status is "Image Scan Status: Failed" with a red warning icon. A red dashed arrow points from this status to the "Criteria Evaluation" table below. The table has columns for QIDs, CVEs, Software, and five severity levels (Severity 5 to Severity 1). The "Criteria Evaluation" row shows red 'X' marks for QIDs, CVEs, and Software, and green checkmarks for Severity 5, Severity 4, Severity 2, and Severity 1. Below the table are four charts: "Vulnerabilities Trend" (a bar chart comparing current build to build #124), "Confirmed Vulnerabilities (33)" (a donut chart showing 33 total, with 32 being Severity 3), "Potential Vulnerabilities (1)" (a donut chart showing 1 total, with 0 being Severity 5, 0 being Severity 4, 0 being Severity 3, 1 being Severity 2, and 0 being Severity 1), and "Patchability" (a donut chart showing 31 Yes and 3 No).

	QIDs	CVEs	Software	Severity 5	Severity 4	Severity 3	Severity 2	Severity 1
Criteria Evaluation	✗	✗	✗	✓	✓	✗	✓	✓

*Excluded QIDs: 176197

✗ Violates criteria ✓ Satisfies criteria **Not Configured