

Fortify Scan Issue: Buildable source not delivered



This page has been made public for vendors

Question

What does the Fortify scan issue "Buildable source not delivered" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that it does not appear that the full buildable source code was delivered. This may be based on a judgment call by the reviewer based on the detection steps below. This makes it difficult to determine if scan meets the requirement that the correct source was scanned.

How to detect

If the source code is not present in the V&V secure code review package, this is an issue.

More likely, however, this will be detected because the delivered code *exactly* matches the scanned code which may mean the code that was delivered was the code exported from Fortify instead of the full buildable source. Detect this issue by comparing the code to be delivered to the code that was scanned by Fortify. The following steps may be performed to compare the two sets of code:

1. Export the code from the FPR file - this will correspond to the code files that were scanned
 - a. Open the FPR in Audit Workbench
 - b. Select the Tools -> Extract Source Code menu item
 - c. Select the folder to export the code to
2. Compare the extracted code to the source code distribution supplied as part of the secure code review package. You can use WinMerge, diff, or other appropriate application.
 - a. If there are no differences between the code to be delivered and the code to be scanned, then it may be an indication of an issue. While the code files should be the same, usually the delivered source will also include build files, graphics files, and a variety of other non-code supporting files.

How to resolve

Deliver the full buildable source code directory that was scanned with Fortify including all source files and non-source supporting files. Do not deliver the exported source code from Fortify. If the full source does not have any non-code files, include a readme file with an explanation of why there are no non-code files and that will be taken into consideration when reviewing the code.

References

- [VA Top 10 Fortify Scan Issues For 2016 \(Q3\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q4\)](#)

HPE Fortify Version	4.30 and later
Programming Language	<input checked="" type="checkbox"/> C/C++ <input checked="" type="checkbox"/> .NET <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Objective-C <input checked="" type="checkbox"/> Other
Fortify Audit Workbench	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Fortify IDE Plugin	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Other Fortify Component	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Request code review tools, validations, and support [HERE](#).