

Fortify Scan Issue: Cannot determine what source code provided corresponds to source code scanned



This page has been made public for vendors

Question

What does the Fortify scan issue "Cannot determine what source code provided corresponds to source code scanned" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that there were problems comparing the scanned source code to the delivered source code because the directory structures of the two do not match. This makes it difficult to determine if scan meets the requirement that the correct source was scanned.

How to detect

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. Look to make sure the directory structure and location of code in that structure is the same between both versions of code. They should be the same, but if they differ greatly then the review will likely not be able to compare the two.

How to resolve

If the directory structure or location of files differs greatly between the scanned and delivered source code, the difference must be resolved. Either the code must be rescanned to match the delivered code or the delivered source code must be modified to match the scanned code. The appropriate action depends on which version will be the production version of the code.

References

- [VA Top 10 Fortify Scan Issues For 2016 \(Q2\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q4\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q1\)](#)

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](#).