

Fortify Scan Issue: Code scanned but not delivered



This page has been made public for vendors

Question

What does the Fortify scan issue "Code scanned but not delivered" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that code files were included in the Fortify scan but not included in the delivered code. When source code files are scanned, but not included in the distribution package, it's not clear if findings associated with the extra files need to be analyzed and remediated or if the files were simply omitted from what was delivered and planned for production.

How to detect

Detect this issue by comparing the code to be delivered to the code that was scanned by Fortify. This ensures that all the source code has been scanned and the version that was scanned is the version that is to be deployed. 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 for source code files in the scanned files that are not in the distribution package.

How to resolve

For any code files that are scanned, but not delivered perform the following as appropriate:

- Rescan the code and remove files that should not be in the production build
- Deliver the code that was scanned
- Include a file with the code review package that indicates why there is a discrepancy

References

- [VA Top 10 Fortify Scan Issues For 2016 \(Q4\)](#)
- [VA Top 10 Fortify Scan Issues For 2016 \(Q3\)](#)
- [VA Top 10 Fortify Scan Issues For 2016 \(Q2\)](#)
- [VA Top 10 Fortify Scan Issues For 2016 \(Q1\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q4\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q3\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q2\)](#)

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](#).