

How to Proceed with a Secure Code Review Validation Report with Orange Warnings



This page has been made public for vendors

Question

I recently submitted my application for a V&V secure code review validation. The residual findings sections of the report have a large orange box with the following warning:

"WARNING: The V&V Secure Code Review Validation Process has encountered blocking issues, current scan results should not be relied upon."

What do I do next to resolve this problem?

Answer

The warning indicates that there were a number of unresolved scan issues noted which may affect the results reported by Fortify. The results of the current scan are therefore not a reliable indication of the security vulnerabilities that may exist in the system. A description of the issues that are resulting in the warning are explained in section 4.5 Unresolved Scan Issue Findings in the report. Additional information to support these findings may be provided in appendices referenced in the descriptions of each scan issue.

Your goal as the application developer should be to perform the same or similar types of analysis of your final scan, as what is explained in Section 3.1, Validation Strategy, of the V&V Secure Code Review Report Template, before resubmitting your application. A description of how to perform these analyses is provided in the technical note [How to Validate a V&V secure code review package](#). You also need to address the issues observed in the report. If you are not the developer, it is your responsibility to obtain development resources to make fixes.

Descriptions of how to detect and remediate most common scan issues are collected in the technical notes: [Common Fortify Scan Issues](#).

Next steps for when you have determined that issues identified in the report have been addressed and that your application is ready for a follow-on validation, you will need to open a new NSD ticket and follow the same procedures as the original attempted review [here](#).

For more information about Accreditation Requirements, contact the VA Certification Program Office (CPO) at CertificationPMO@va.gov to review the accreditation requirements with an Office of Cyber Security (OCS) CPO resource.

References

- [VA Secure Code Review Standard Operating Procedures \(SOP\)](#)
- [VA Accreditation Requirements Guide SOP](#)
- [How to Validate a V&V secure code review package](#)
- [Common Fortify Scan Issues](#)



System Owner tips

If a report with warnings was returned,

... there is a problem. You need to follow up with the developer to ensure that issues identified in the report are addressed, and then ensure that a follow-on V&V secure code review validation is performed.

If a report without warnings was returned,

... there may still be a problem. You need to check the report to see if there are any critical, high, or scan findings that the developer did not fix, and then ensure that a follow-on V&V secure code review validation is performed if necessary.

If a report was returned with residual findings,

... it is your responsibility to follow up with the developer to create and implement a Plan of Action and Milestones (POAM) to make fixes to application source code and to ensure that follow-on V&V secure code review validations are performed as necessary.