

VA Software Assurance Secure Coding Tip

Old Versions of Rulepacks May Leave Vulnerabilities Undetected

This week's Secure Coding Tip is about using old versions of rulepacks during scans when using the HPE Fortify Static Code Analyzer (SCA) software. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [1], and enforced as part of the ATO issuance process.[2]

One of the top 10 issues[3] encountered by VA application developers using the HPE Fortify SCA software is using old versions of rulepacks during a scan.[4] The rulepacks encode the security knowledge that Fortify applies to the code. Scans that do not use the most recent rulepacks may not therefore include a complete set of results.

There are several steps you can take to resolve the issue.

[Read more...](#)

[1] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.

[2] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.

[3] [VA Top 10 Fortify Scan Issues For 2016 \(Q4\)](#)

[4] [VA Top 10 Fortify Scan Issues For 2016 \(Q4\), S4: Old version of rulepacks used during scan](#)

Resources

- [VA Software Assurance Support Site](#)
- [Request VA-licensed code review tools, validations, and support](#)
- [Latest VA Software Assurance Program Office announcements](#)
- [Check if your application has been registered \(internal link\)](#)

Reminders

- [The next working group meeting is on 11/8](#)

You have received this message because you are subscribed to VA Software Assurance Working Group. To unsubscribe to these announcements or to subscribe, email: OISSwASupportGroup@va.gov

VA



**U.S. Department
of Veterans Affairs**

**Office of Information
and Technology**

*Software Assurance
Program Office*