OFFICE OF
INFORMATION
SECURITY

Secure Code Review Validation Report

[Application Name] [Application Version]

[MONTH] [DAY], [YEAR]

Office of Information Security

SOFTWARE ASSURANCE PROGRAM OFFICE

Table of Contents

1. Secure Code Review Validation Report Introduction 1
   1.1 Application Information 1
2. Secure Code Review Validation Results 3
3. Secure Code Review Validation Process Details 4
   3.1 Validation Strategy 4
   3.2 Tools Used for Validation 5
   3.3 Categorization of Findings 5
4. Secure Code Review Validation Findings and Recommendations 7
   4.1 Residual Critical Findings (xx Total) 7
   4.2 Residual High Findings ([#] Total) 7
   4.3 Residual Medium Findings ([#] Total) 7
   4.4 Residual Low Findings ([#] Total) 8
   4.5 Unresolved Scan Issue Findings ([#] Total) 8
   4.6 Additional Findings ([#] Total) 9
      4.6.1 CWE-[id] ([#] Instances) 10
5. Secure Code Review Validation Report Conclusion 11
   5.1 Resources that you may find helpful 11

Table of Figures

Figure 1. Summary of Residual Vulnerabilities & Unresolved Scan Issues 3

1. Secure Code Review Validation Report Introduction

This document contains the results of the validation by the VA Office of Information Security (OIS) Software Assurance (SwA) Program Office of a secure code review of [application name] performed by the developer.

This document contains the following additional sections:

Section 2. Secure Code Review Validation Results

This section summarizes the results of the validation of the developer secure code review.

Section 3. Secure Code Review Validation Process Details

This section describes how the validation of the developer secure code review was performed.

Section 4. Secure Code Review Validation Findings and Recommendations

This section provides residual secure code review validation findings that should have already been fixed prior to the validation.[1] Recommendations are also provided.

Section 5. Secure Code Review Validation Report Conclusion

This section provides additional recommendations to build security in during development.

1.1 Application Information

The version of [application name] for which static analysis tool scan results was [application version]. The following was provided by the developer for review:

1. Completed V&V Secure Code Review / IV&V High-Risk & High-Priority Application Review Request Form
2. [file name] HP Fortify Static Code Analyzer (SCA) static analysis tool scan result file
3. [file name] HP Fortify SCA static analysis tool custom rule file

---

[1] *Per VA OIS Secure Code Review Standard Operating Procedures (SOP) which can be downloaded from https://wiki.mobilehealth.va.gov/display/OISSWA/Public+Document+Library*

4. [upload location] [application name] [application version] source code

2. Secure Code Review Validation Results

This document contains the results of a Verification and Validation (V&V) review, conducted by the VA OIS SwA Program Office, of developer-provided HP Fortify SCA static analysis tool scan result files. And, of any provided custom scan tool custom rule files, as well as the [application name] [application version] source code. Goals of performing secure code reviews at the VA include ensuring that risk-based activities in applications are performed in a secure manner. Goals of V&V secure code review validations include ensuring that secure code reviews performed by VA software developers have been done correctly and consistently.

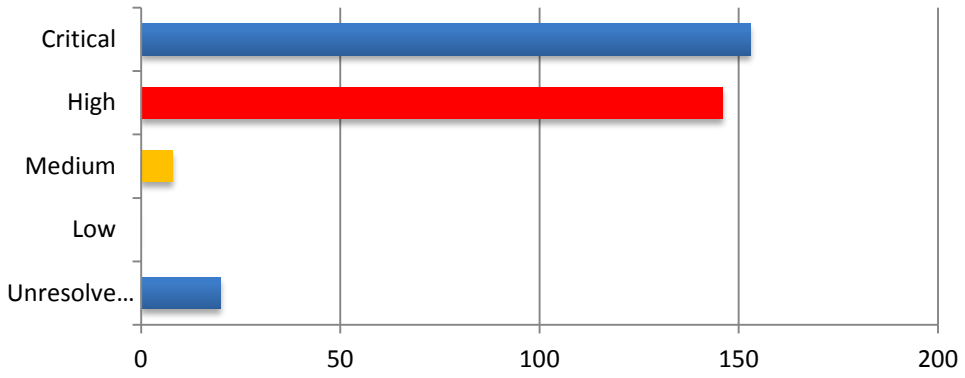
The V&V secure code review validation conducted by the VA OIS SwA Program Office covered provided materials to ensure that:

1. Application information in secure code review validation request packages is accurate and complete, and
2. Application scan results demonstrate that VA standards have been met , and
3. Application scan results demonstrate that mitigations must have been made for issues reported by the HP Fortify SCA static analysis tool, and
4. There are justifications provided for cases where HP Fortify SCA static analysis tool rules are disabled, or scan results are marked as false positives.

For more information about the validation process, see Section 3.

The V&V secure code review validation conducted by the VA OIS SwA Program Office identified a total of [count] residual vulnerabilities that were considered Critical in severity. There were a total of [count] residual High severity vulnerabilities. There were a total of [count] residual Medium severity vulnerabilities. There were a total of [count] residual Low severity vulnerabilities. There were a total of [count] unresolved scan issues.

Figure 1. Summary of Residual Vulnerabilities & Unresolved Scan Issues



For more information about residual vulnerabilities and unresolved scan issues that were identified during the secure code review validation, see Section 4.

3. Secure Code Review Validation Process Details

The secure code review validation was performed overall as follows:

Step 1. Perform initial planning

The first step that was performed was to perform initial planning. This included developing a strategy for performing the review and identifying considerations that should be taken into account during the review, such as any HP Fortify SCA static analysis tool custom rule files provided by the developer.

Step 2. Review source code

The next step is to perform the review. A combination of using HP Fortify SCA to review scan result files and manual analysis was used. The scan results were reviewed to ensure that best practices for performing secure code review have been followed, and that VA standards have been met, as noted in the previous section.

Step 3. Write report

The last step in the secure code review validation process is to write up the report, after working with the VA application developer to resolve any issues identified during review.

3.1 Validation Strategy

The secure code review validation was performed by reviewing HP Fortify SCA static analysis tool scan result files and any provided HP Fortify SCA static analysis tool custom rule files. The provided source code was reviewed as need to support analysis of the provided scan result and custom rule files. The secure code review validation included at a minimum the following checks:

Review developer-provided scan file for matching source code

This validation check consists of ensuring that the source code matches the uploaded static analysis tool scan result files. While during the comparison there may be some differences such as build files, source code files should not contain any differences.

Review developer-provided scan file for scanning issues

This validation check consists of reviewing static analysis tool scan result file for any anomalies in the scan. When running the scan there may have been issues reported by the static analysis tool that affected the quality or completeness of the scan that may have been overlooked.

Review developer-provided scan file for residual findings

This validation check consists of ensuring that there are no Critical or High findings in the uploaded static analysis tool scan result file (HP Fortify SCA ".fpr" extension file) using Fortify Audit Workbench, after first configuring it to use any provided custom rule files.

Review developer-provided scan file for suppression of issues

This validation check consists of reviewing static analysis tool scan result files to ensure that issues reported by HP Fortify SCA have not been suppressed, as opposed to adding comments and developing custom rules as might be appropriate.

Review developer-provided custom rule files, if provided

This validation check consists of reviewing any provided static analysis tool custom rule files. Analysis includes examining custom rule files e.g. to ensure that there are no rules to disable built-in Fortify rules, unless those custom rules include documentation justifying their use.

Perform additional supporting analysis, as needed

This validation check consists of performing additional supporting analysis for items that may have been identified during the course of the validation for a particular application. For example, findings in the scan result files have been marked as N/A, checks would be performed to ensure there is some documented justification, and to verify the soundness of the justification. Alternately for example, analysis may be performed to determine the appropriateness of exclusions.

3.2 Tools Used for Validation

The VA OIS SwA Program Office uses the same static analysis tool (HP Fortify SCA) as VA application developers. The same static analysis tool is used in order to confidence in the outcome of the secure code review validation if the tool is in fact being used during development. HP Fortify SCA version [version] was used to review provided static analysis tool scan result and custom rule files. The Audit Workbench tool which is part of HP Fortify SCA was used to facilitate examining static analysis tool scan result files. Similarly, the Custom Rules Editor tool which is also part of HP Fortify SCA was used to facilitate examining custom rule files.

3.3 Categorization of Findings

The findings that resulted from performing the secure code review validation are grouped in Section 4 of this report by severity and type of vulnerability. Findings were rated according to

severities reported by the HP Fortify SCA tool, and/or at the discretion of the VA OIS SwA Program Office as follows:

Findings that are Critical in severity

Vulnerabilities in source code that must be fixed immediately, for example exposed passwords or Personally-Identifiable Information (PII).

Findings that are High in severity

Vulnerabilities in source code that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.

Findings that are Medium in severity

Vulnerabilities in source code that provide information that have a high potential of giving access to an intruder.

Findings that are Low in severity

Vulnerabilities in source code that provide information that potentially could lead to compromise.

Findings that are unresolved scan issues

This finding categorization is reserved for issues having to do with how the scan was conducted, for example, source code not matching the upload static analysis tool scan result files.

Additional findings

This finding categorization is reserved for vulnerabilities that were identified manually during the course of the validation while reviewing for other types of potential deficiencies.

4. Secure Code Review Validation Findings and Recommendations

4.1 Residual Critical Findings ([#] Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by HP Fortify SCA that were Critical in severity were left unmitigated.

Or,

The following vulnerabilities identified by HP Fortify SCA that were Critical in severity were left unmitigated and are still being reported by HP Fortify SCA:

CWE-ID	CWE-Title	Number of Instances	Notes

4.2 Residual High Findings ([#] Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by HP Fortify SCA that were High in severity were left unmitigated.

Or,

The following vulnerabilities identified by HP Fortify SCA that were High in severity were left unmitigated and are still being reported by HP Fortify SCA:

CWE-ID	CWE-Title	Number of Instances	Notes

4.3 Residual Medium Findings ([#] Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by HP Fortify SCA that were Medium in severity were left unmitigated.

Or,

The following vulnerabilities identified by HP Fortify SCA that were Medium in severity were left unmitigated and are still being reported by HP Fortify SCA:

CWE-ID	CWE-Title	Number of Instances	Notes

4.4 Residual Low Findings ([#] Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by HP Fortify SCA that were Low in severity were left unmitigated.

Or,

The following vulnerabilities identified by HP Fortify SCA that were Low in severity were left unmitigated and are still being reported by HP Fortify SCA:

CWE-ID	CWE-Title	Number of Instances	Notes

4.5 Unresolved Scan Issue Findings ([#] Total)

Based on the information provided, it does not appear that there were issues when the scan of the source code was conducted.

Or,

Description of Concern
There are issues having to do with how the scan was conducted by the developer that were not able to be resolved during the course of the review. These issues may have impacted the ability of HP Fortify SCA to identify Critical, High, Medium, or Low in severity findings. Descriptions of unresolved scan issues, and recommendations for each, are below.

Details

	Issue	***Description***	***Recommendation***
1.	Suppression of issues	Developer has suppressed issues reported by HP Fortify SCA.	Un-suppress issues, and add comments and develop custom rules as might be appropriate to justify identifying findings as false positives.
2.			
3.			
4.			

4.6 Additional Findings ([#] Total)

There were no additional findings that were identified during the course of the validation.

Or,

CWE-ID	Residual Vulnerability Severity	CWE Title
4.6.1 CWE-[id] ([#] Instances)	Medium	[title]

Description of Concern

There are concerns related to [title] (CWE-[id]). Individual instances that were found during the secure code review are below. A code example, description of potential impact, and recommendations follow.

Location

	Directory	*File*	*Line*
1.			
2.			
3.			
4.			

Code Example

A code example from a residual vulnerability is below. In the example, [provide a code snippet and a brief description].

```
...
string strPassPhrase = "[redacted]";
...
```

Impact

[Provide description of impact]

Remediation

[Provide remediation advice]

5. Secure Code Review Validation Report Conclusion

Writing secure code is every VA application developer's responsibility. Secure code reviews have been included as activities in the VA ProPath System Development Life Cycle (SDLC) Product Build (BLD) processes since ProPath Release 16.5. Fortify should be used according to the VA OIS Secure Code Review Standard Operating Procedures (SOP). The VA OIS SwA Program Office uses the same static analysis tool (HP Fortify SCA) as VA application developers. The same static analysis tool is used in order to confidence in the outcome of V&V secure code review validations, assuming the tool is being used during development.

If a Temporary Authority to Operate (TATO) is granted, it is recommended that vulnerabilities are remediated within the time frames below:

- Critical & Scan Issues – Must be remediated immediately.
- High – Must be remediated within 60 days.
- Medium –Must be remediated within 90 days.
- Low – Must be remediated according to the timeframe established by the system owner.

Per direction of VA management, if the Software Assurance Program Office's assessment of security controls for this application triggered the need for a POAM, then the POAM vulnerability item must be kept open and tracked until the vulnerability has been mitigated or remediated.

Failure to comply with remediation instructions shall result in reporting the issue to the CISO for further action, which may include disabling access to the application. ISOs and system owners that cannot comply with these timelines must submit a Risk Based Decision (RBD) memorandum through the Software Assurance Program Office.

5.1 Resources that you may find helpful

VA OIS Software Assurance Program Office support site:

https://wiki.mobilehealth.va.gov/display/OISSWA

VA OIS Secure Code Review Standard Operating Procedures (SOP):

https://wiki.mobilehealth.va.gov/display/OISSWA/Public+Document+Library

Fortify product documentation:

This is included as part of Fortify software distribution.

OWASP Top Ten:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CWE/SANS TOP 25:

https://cwe.mitre.org/top25