Fortify Security Report

2019/1/16

Executive Summary

Issues Overview

On 2019/1/16, a source code review was performed over the 999 code base. 2 files, 4 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 4 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
Low	4

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location:
Number of Files: 2
Lines of Code: 4
Build Label: <No Build Label>

Scan Information

Scan time: 00:18
SCA Engine version: 18.20.1071
Machine Name: TWTPETCFS
Username running scan: administrator

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Command Line Arguments:
null.HelloWorld.main

Filter Set Summary

Current Enabled Filter Set:
Security Auditor View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low

Audit Guide Summary

Audit guide not enabled

Results Outline

Overall number of results

The scan found 4 issues.

Vulnerability Examples by Category

Issue Count by Category	
Issues by Category	
J2EE Bad Practices: Leftover Debug Code	2
Poor Logging Practice: Use of a System Output Stream	2

Issue Breakdown by Analysis

Issues by Analysis