



Fortify Security Report

Jan 23, 2020

pgupta25

Executive Summary

Issues Overview

On Jan 23, 2020, a source code review was performed over the event code base. 38 files, 519 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 0 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order

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: /srv/openmrs_code/org/openmrs/module/event

Number of Files: 38

Lines of Code: 519

Build Label: <No Build Label>

Scan Information

Scan time: 00:59

SCA Engine version: 19.1.0.2241

Machine Name: vclv99-89.hpc.ncsu.edu

Username running scan: pgupta25

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:

System Information:

null.null.null

java.lang.Throwable.getMessage

Filter Set Summary

Current Enabled Filter Set:

Quick 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

Visibility Filters:

If impact is not in range [2.5, 5.0] Then hide issue

If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

Results Outline

Overall number of results

The scan found 0 issues.

Vulnerability Examples by Category

Detailed Project Summary

Files Scanned

Code base location: /srv/openmrs_code/org/openmrs/module/event

Files Scanned:

.travis.yml yml Dec 13, 2019 12:56:26 PM
 api/pom.xml xml 4.4 KB Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/Event.java java 16 Lines 5.2 KB Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/EventClassScanner.java java 16 Lines 3.1 KB Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/EventEngine.java java 98 Lines 12.1 KB Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/EventListener.java java Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/EventMessage.java java 2 Lines Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/SubscribableEventListener.java java 1 KB Dec 13, 2019 12:56:26 PM
 api/src/main/java/org/openmrs/event/api/db/hibernate/HibernateEventInterceptor.java java 61 Lines 8.7 KB Dec 13, 2019 12:56:26 PM
 api/src/main/resources/messages.properties java_properties Dec 13, 2019 12:56:26 PM
 api/src/main/resources/messages_es.properties java_properties Dec 13, 2019 12:56:26 PM
 api/src/main/resources/messages_fr.properties java_properties Dec 13, 2019 12:56:26 PM
 api/src/main/resources/moduleApplicationContext.xml xml 1.2 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/EventClassScannerTest.java java 6 Lines 1.3 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/EventEngineUtil.java java 3 Lines Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/EventMessageListener.java java 8 Lines 1.2 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/EventTest.java java 125 Lines 12.1 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/MockEventListener.java java 25 Lines 3.2 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/MockNestedService.java java Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/event/MockNestedServiceImpl.java java 6 Lines 1.2 KB Dec 13, 2019 12:56:26 PM
 api/src/test/java/org/openmrs/module/event/advice/EventBehaviorTest.java java 88 Lines 10.5 KB Dec 13, 2019 12:56:26 PM
 api/src/test/resources/TestingApplicationContext.xml xml 2.3 KB Dec 13, 2019 12:56:26 PM
 api/target/classes/messages.properties java_properties Dec 18, 2019 3:36:12 PM
 api/target/classes/messages_es.properties java_properties Dec 18, 2019 3:36:12 PM
 api/target/classes/messages_fr.properties java_properties Dec 18, 2019 3:36:12 PM
 api/target/classes/moduleApplicationContext.xml xml 1.2 KB Dec 18, 2019 3:36:12 PM
 api/target/maven-archiver/pom.properties java_properties Dec 18, 2019 3:36:15 PM
 omod/pom.xml xml 4.8 KB Dec 13, 2019 12:56:26 PM
 omod/src/main/java/org/openmrs/module/event/EventActivator.java java 20 Lines 2.9 KB Dec 13, 2019 12:56:26 PM
 omod/src/main/resources/config.xml xml 1.1 KB Dec 13, 2019 12:56:26 PM
 omod/src/main/resources/webModuleApplicationContext.xml xml 1.3 KB Dec 13, 2019 12:56:26 PM
 omod/src/test/java/org/openmrs/module/event/EventActivatorTest.java java 45 Lines 5.1 KB Dec 13, 2019 12:56:26 PM
 omod/target/classes/config.xml xml 1 KB Dec 18, 2019 3:36:18 PM
 omod/target/classes/webModuleApplicationContext.xml xml 1.3 KB Dec 18, 2019 3:36:18 PM
 omod/target/event-2.7.0/config.xml xml 1 KB Dec 18, 2019 3:36:19 PM
 omod/target/event-2.7.0/webModuleApplicationContext.xml xml 1.3 KB Dec 18, 2019 3:36:19 PM
 omod/target/maven-archiver/pom.properties java_properties Dec 18, 2019 3:36:19 PM
 pom.xml xml 4.5 KB Dec 13, 2019 12:56:26 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Core, Java

Version: 2019.4.0.0009

ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF

SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, Annotations

Version: 2019.4.0.0009

ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B

SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, Android

Version: 2019.4.0.0009

ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952

SKU: RUL13093

Name: Fortify Secure Coding Rules, Extended, Configuration

Version: 2019.4.0.0009

ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56

SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Java

Version: 2019.4.0.0009

ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317

SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, Content

Version: 2019.4.0.0009

ID: 9C48678C-09B6-474D-B86D-97EE94D38F17

SKU: RUL13067

Name: Fortify Secure Coding Rules, Core, Golang

Version: 2019.4.0.0009

ID: 1DCE79F8-AF6B-474D-A05A-5BFFC8B13DCD

SKU: RUL13218

Name: Fortify Secure Coding Rules, Extended, JSP

Version: 2019.4.0.0009

ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2

SKU: RUL13026

External Metadata:

Version: 2019.4.0.0009

Name: CWE

ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC

The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019

ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE

The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2

ID: 7F037130-41E5-40F0-B653-7819A4B3E241

The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.

The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA

ID: B40F9EE0-3824-4879-B9FE-7A789C89307C

The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR

ID: 771C470C-9274-4580-8556-C12F5E4BEC51

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or

to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012

ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506

Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008

ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA

The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules also reflect security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanism with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4

ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0

NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP Mobile 2014

ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE

The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004

ID: 771C470C-9274-4580-8556-C023E4D3ADB4

The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007

ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A

The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010

ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59

The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013

ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4

The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017

ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248

The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1

ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531

The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2

ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5

Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0

ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E

The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0

ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1

ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2

ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1

ID: EADE255F-6561-4EFE-AD31-2914F6BFA329

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0

ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74

The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009

ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8

The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010

ID: 72688795-4F7B-484C-88A6-D4757A6121CA

SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (<http://cwe.mitre.org/>). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011

ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63

SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (<http://cwe.mitre.org/>). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1

ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7

Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10

ID: 788A87FE-C9F9-4533-9095-0379A9B35B12

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4

ID: 58E2C21D-C70F-4314-8994-B859E24CF855

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

- CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- CAT II: provide information that have a high potential of giving access to an intruder.
- CAT III: provide information that potentially could lead to compromise.

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5

ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

- CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- CAT II: provide information that have a high potential of giving access to an intruder.
- CAT III: provide information that potentially could lead to compromise.

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6

ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

- CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- CAT II: provide information that have a high potential of giving access to an intruder.
- CAT III: provide information that potentially could lead to compromise.

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7

ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

- CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- CAT II: provide information that have a high potential of giving access to an intruder.
- CAT III: provide information that potentially could lead to compromise.

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9

ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1

ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10

ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2

ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden

or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3

ID: A0B313F0-29BD-430B-9E34-6D10F1178506

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4

ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5

ID: E6010E0A-7F71-4388-B8B7-EE9A02143474

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority

Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6

ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7

ID: B04A1E01-F1C1-48D3-A827-0F70872182D7

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
- existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8

ID: E6805D9F-D5B5-4192-962C-46828FF68507

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-*ID*: CAT *SEV*]. DISA STIG defines three severities with respect to vulnerabilities where their:

- exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
- exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).

existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).
exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).
existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties
WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.X11.XToolkit
com.fortify.AuthenticationKey=/home/pgupta25/.fortify/config/tools
com.fortify.Core=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core
com.fortify.InstallRoot=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0
com.fortify.InstallationUserName=pgupta25
com.fortify.SCAExecutablePath=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/bin/sourceanalyzer
com.fortify.TotalPhysicalMemory=8363917312
com.fortify.VS.RequireASPPrecompilation=true

```
com.fortify.WorkingDirectory=/home/pgupta25/.fortify
com.fortify.locale=en
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=event
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.f
ortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.Micr
osoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.com
pilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.co
mpilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer
com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settin
gs,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshhtml,vbhtml,inc,asp,vbscript,js,ini,bas,cls
,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,
wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,conf,json,yaml,yml
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/rules
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICG
Builder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuild
er,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PH
PLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFileDir=/home/pgupta25/.fortify/sca19.1/log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=/home/pgupta25/.fortify/sca19.1/log/sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
```

```
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshhtml,vbhtml
com.fortify.sca.PID=5044
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.ProjectRoot=/home/pgupta25/.fortify
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=/srv/openmrs_code/org/openmrs/module/event/event_scan.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=PLSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs
com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fi
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
```

com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.cpfe.441.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP
com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP

com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4
com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-

```
names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
file.encoding=UTF-8
file.encoding.pkg=sun.io
file.separator=/
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.print.PSPrinterJob
java.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/endorsed
java.ext.dirs=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/ext:/usr/java/packages/lib/ext
java.home=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre
java.io.tmpdir=/tmp
java.library.path=/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/config/log4j2.xml
log4j.isThreadContextMapInheritable=true
max.file.path.length=255
os.arch=amd64
os.name=Linux
os.version=4.15.0-58-generic
path.separator=:
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/resources.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/
jre/lib/rt.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/sunrsasign.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/j
sse.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jce.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/charsets.jar:/
opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/jfr.jar:/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/classes
```

```
sun.boot.library.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/jre/lib/amd64
sun.cpu.endian=little
sun.cpu.isalist=
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -
XX:SoftRefLRUPolicyMSPerMB=3000 -Dcom.fortify.sca.env.exesearchpath=/sbin:/bin:/usr/bin:/usr/local/bin -
Dcom.fortify.sca.ProjectRoot=/home/pgupta25/.fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=5044 -
Xmx4096M -Dcom.fortify.TotalPhysicalMemory=8363917312 -Xss16M -Dcom.fortify.sca.JVMArgs=-
XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx4096M -Xss16M -
Djava.class.path=/opt/Fortify/Fortify_SCA_and_Apps_19.1.0/Core/lib/exe/sca-exe.jar -scan
@/home/pgupta25/.fortify/Eclipse.Plugin-19.1.0/event/eventScan.txt
sun.jnu.encoding=UTF-8
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=unknown
user.country=US
user.dir=/home/pgupta25
user.home=/home/pgupta25
user.language=en
user.name=pgupta25
user.timezone=America/New_York
```

Commandline Arguments

```
-scan
-b
event
-format
fpr
-machine-output
-f
/srv/openmrs_code/org/openmrs/module/event/event_scan.fpr
```

Warnings

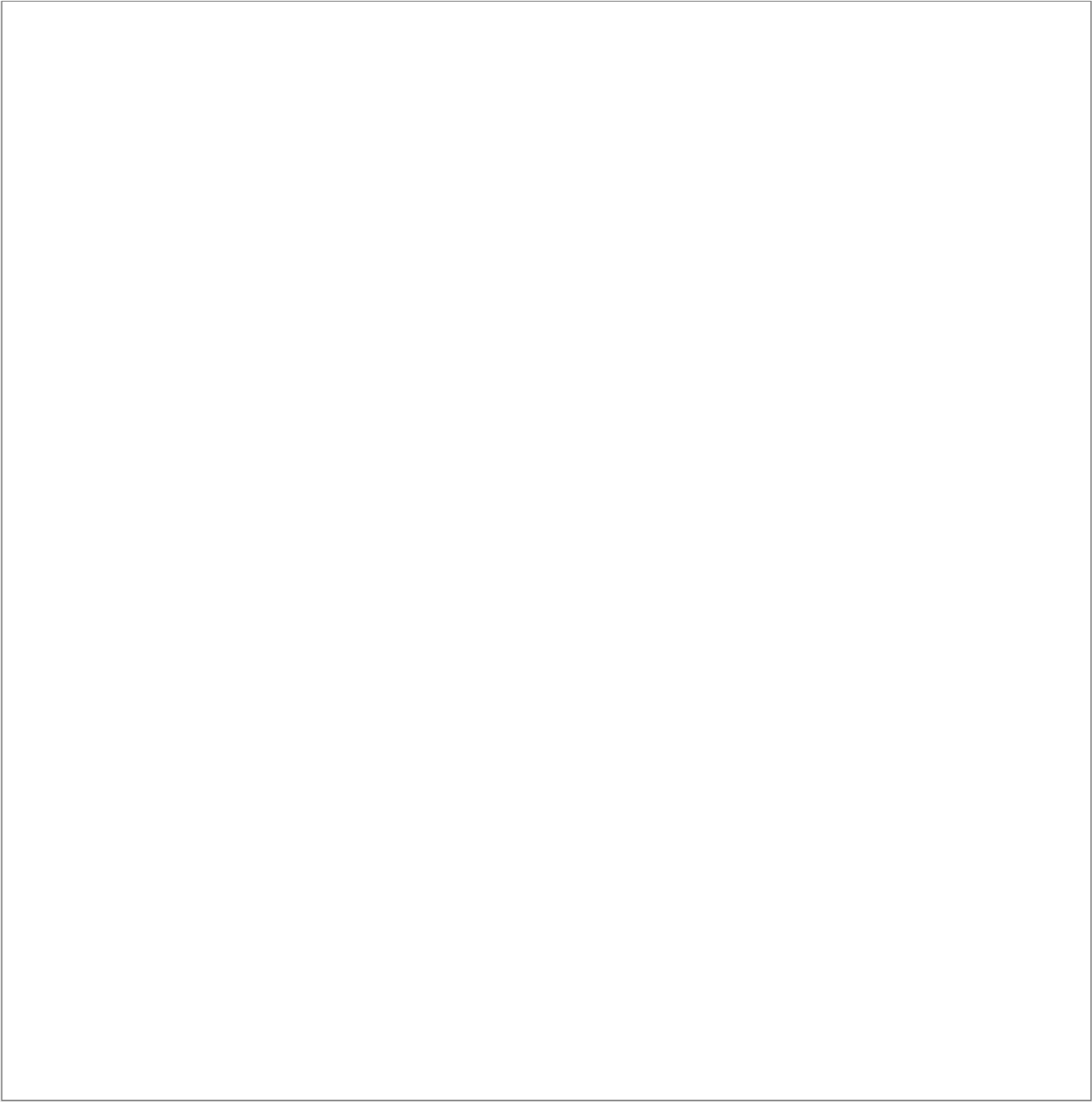
[12003] Assuming Java source level to be 1.8 as it was not specified. Note that the default value may change in future versions.

Issue Count by Category

Issues by Category

Issue Breakdown by Analysis

Issues by Analysis



Issues by New Issue