|  |
| --- |
| stms  Branch : main  Version 1.0  Code analysis |

|  |
| --- |
| **By: Administrator**  **2025-04-11** |

# Content

[Content 1](#_Toc97156258)

[Introduction 2](#_Toc97156259)

[Configuration 2](#_Toc97156260)

[Synthesis 3](#_Toc97156261)

[Analysis Status 3](#_Toc97156262)

[Quality gate status 3](#_Toc97156263)

[Metrics 3](#_Toc97156264)

[Tests 3](#_Toc97156265)

[Detailed technical debt 3](#_Toc97156266)

[Metrics Range 5](#_Toc97156267)

[Volume 5](#_Toc97156268)

[Issues 6](#_Toc97156269)

[Charts 6](#_Toc97156270)

[Issues count by severity and type 8](#_Toc97156271)

[Issues List 8](#_Toc97156272)

[Security Hotspots 9](#_Toc97156273)

[Security hotspots count by category and priority 9](#_Toc97156274)

[Security hotspots List 9](#_Toc97156275)

# Introduction

This document contains results of the code analysis of stms.

# Configuration

* Quality Profiles
  + Names: Sonar way [CSS]; Sonar way [Java]; Sonar way [XML];
  + Files: 12bd25e4-800a-4dcb-9a6e-6c8b7342f1ac.json; 515ecee0-d2e2-438a-81d7-53e17247e347.json; 9c84b27d-a3cb-4611-8b72-e28f331adc62.json;
* Quality Gate
  + Name: Sonar way
  + File: Sonar way.xml

# Synthesis

## Analysis Status

|  |  |  |  |
| --- | --- | --- | --- |
| Reliability | Security | Security Review | Maintainability |
| C.png | **A.png** | **E.png** | **A.png** |

## Quality gate status

|  |  |
| --- | --- |
| Quality Gate Status | **OK.png** |



## Metrics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Coverage | Duplication | Comment  density | Median number of lines of code per file | Adherence to coding standard |
| 10.0 % | **15.1 %** | **1.3 %** | **68.0** | **98.7 %** |

## Tests

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Total | Success Rate | Skipped | Errors | Failures |
| 38 | **100.0 %** | **0** | **0** | **0** |

## Detailed technical debt

|  |  |  |  |
| --- | --- | --- | --- |
| Reliability | Security | Maintainability | Total |
| 0d 2h 5min | - | 6d 1h 58min | 6d 4h 3min |

## Metrics Range

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Cyclomatic  Complexity | Cognitive  Complexity | Lines of code per file | Comment  density (%) | Coverage | Duplication (%) |
| Min | 0.0 | 0.0 | 3.0 | 0.0 | 0.0 | 0.0 |
| Max | 1211.0 | 717.0 | 8258.0 | 20.4 | 100.0 | 69.8 |

## Volume

|  |  |
| --- | --- |
| Language | Number |
| CSS | 308 |
| Java | 7912 |
| XML | 38 |
| Total | 8258 |

# Issues

## Charts

## Issues count by severity and type

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type / Severity | INFO | MINOR | MAJOR | CRITICAL | BLOCKER |
| BUG | 0 | 2 | 7 | 0 | 0 |
| VULNERABILITY | 0 | 0 | 0 | 0 | 0 |
| CODE\_SMELL | 6 | 60 | 82 | 102 | 0 |

## Issues List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Severity | Number |
| "InterruptedException" and "ThreadDeath" should not be ignored |  | BUG | MAJOR | 7 |
| "equals(Object obj)" and "hashCode()" should be overridden in pairs |  | BUG | MINOR | 1 |
| Double Brace Initialization should not be used |  | BUG | MINOR | 1 |
| Methods should not be empty |  | CODE\_SMELL | CRITICAL | 2 |
| String literals should not be duplicated |  | CODE\_SMELL | CRITICAL | 94 |
| "switch" statements should have "default" clauses |  | CODE\_SMELL | CRITICAL | 2 |
| Cognitive Complexity of methods should not be too high |  | CODE\_SMELL | CRITICAL | 4 |
| Track uses of "TODO" tags |  | CODE\_SMELL | INFO | 4 |
| Methods should not perform too many tasks (aka Brain method) |  | CODE\_SMELL | INFO | 1 |
| The Singleton design pattern should be used with care |  | CODE\_SMELL | INFO | 1 |
| Empty blocks should be removed |  | CODE\_SMELL | MAJOR | 1 |
| Standard outputs should not be used directly to log anything |  | CODE\_SMELL | MAJOR | 20 |
| Mergeable "if" statements should be combined |  | CODE\_SMELL | MAJOR | 3 |
| Methods should not have too many parameters |  | CODE\_SMELL | MAJOR | 2 |
| Local variables should not shadow class fields |  | CODE\_SMELL | MAJOR | 5 |
| Utility classes should not have public constructors |  | CODE\_SMELL | MAJOR | 3 |
| Generic exceptions should never be thrown |  | CODE\_SMELL | MAJOR | 14 |
| Unused "private" methods should be removed |  | CODE\_SMELL | MAJOR | 2 |
| Empty arrays and collections should be returned instead of null |  | CODE\_SMELL | MAJOR | 16 |
| Only static class initializers should be used |  | CODE\_SMELL | MAJOR | 1 |
| A field should not duplicate the name of its containing class |  | CODE\_SMELL | MAJOR | 1 |
| Format strings should be used correctly |  | CODE\_SMELL | MAJOR | 6 |
| Raw types should not be used |  | CODE\_SMELL | MAJOR | 3 |
| Methods should not have identical implementations |  | CODE\_SMELL | MAJOR | 5 |
| Method names should comply with a naming convention |  | CODE\_SMELL | MINOR | 2 |
| Class variable fields should not have public accessibility |  | CODE\_SMELL | MINOR | 18 |
| Unnecessary imports should be removed |  | CODE\_SMELL | MINOR | 6 |
| Field names should comply with a naming convention |  | CODE\_SMELL | MINOR | 3 |
| Local variable and method parameter names should comply with a naming convention |  | CODE\_SMELL | MINOR | 18 |
| The default unnamed package should not be used |  | CODE\_SMELL | MINOR | 1 |
| "switch" statements should have at least 3 "case" clauses |  | CODE\_SMELL | MINOR | 1 |
| Loops should not contain more than a single "break" or "continue" statement |  | CODE\_SMELL | MINOR | 1 |
| Private fields only used as local variables in methods should become local variables |  | CODE\_SMELL | MINOR | 5 |
| Lambdas should be replaced with method references |  | CODE\_SMELL | MINOR | 2 |
| Multiple variables should not be declared on the same line |  | CODE\_SMELL | MINOR | 1 |
| Classes should not be empty |  | CODE\_SMELL | MINOR | 1 |
| Regular expression quantifiers and character classes should be used concisely |  | CODE\_SMELL | MINOR | 1 |

# Security Hotspots

## Security hotspots count by category and priority

|  |  |  |  |
| --- | --- | --- | --- |
| Category / Priority | LOW | MEDIUM | HIGH |
| LDAP Injection | 0 | 0 | 0 |
| Object Injection | 0 | 0 | 0 |
| Server-Side Request Forgery (SSRF) | 0 | 0 | 0 |
| XML External Entity (XXE) | 0 | 0 | 0 |
| Insecure Configuration | 11 | 0 | 0 |
| XPath Injection | 0 | 0 | 0 |
| Authentication | 0 | 0 | 0 |
| Weak Cryptography | 0 | 0 | 0 |
| Denial of Service (DoS) | 0 | 0 | 0 |
| Log Injection | 0 | 0 | 0 |
| Cross-Site Request Forgery (CSRF) | 0 | 0 | 0 |
| Open Redirect | 0 | 0 | 0 |
| Permission | 0 | 0 | 0 |
| SQL Injection | 0 | 0 | 0 |
| Encryption of Sensitive Data | 0 | 0 | 0 |
| Traceability | 0 | 0 | 0 |
| Buffer Overflow | 0 | 0 | 0 |
| File Manipulation | 0 | 0 | 0 |
| Code Injection (RCE) | 0 | 0 | 0 |
| Cross-Site Scripting (XSS) | 0 | 0 | 0 |
| Command Injection | 0 | 0 | 0 |
| Path Traversal Injection | 0 | 0 | 0 |
| HTTP Response Splitting | 0 | 0 | 0 |
| Others | 0 | 0 | 0 |

## Security hotspots List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Name | Priority | Severity | Count |
| Insecure Configuration | Delivering code in production with debug features activated is security-sensitive | LOW | MINOR | 11 |