SEI CERT Oracle Coding Standard for Java

The Java rules and recommendations in this wiki are a work in progress and reflect the current thinking of the secure coding community. Because this is a development website, many pages are incomplete or contain errors. As rules and recommendations mature, they are published in report or book form as official releases. These releases are issued as dictated by the needs and interests of the secure software development community.

Create a sign-in account if you want to comment on existing content. If you wish to be more involved and directly edit content on the site, you still need to request edit privileges.

Content by label
There is no content with the specified labels

Recommendations

- Rec. 00. Input Validation and Data Sanitization (IDS)
- Rec. 01. Declarations and Initialization (DCL)
- Rec. 02. Expressions (EXP)
- Rec. 03. Numeric Types and Operations (NUM)
- Rec. 04. Characters and Strings (STR)
- Rec. 05. Object Orientation (OBJ)
- Rec. 06. Methods (MET)
- Rec. 07. Exceptional Behavior (ERR)
- Rec. 08. Visibility and Atomicity (VNA)
- Rec. 09. Locking (LCK)
- Rec. 10. Thread APIs (THI)
- Rec. 11. Thread Pools (TPS)
- Rec. 12. Thread-Safety Miscellaneous (TSM)
- Rec. 13. Input Output (FIO)
- Rec. 14. Serialization (SER)
- Rec. 15. Platform Security (SEC)
- Rec. 16. Runtime Environment (ENV)
- Rec. 17. Java Native Interface (JNI)
- Rec. 49. Miscellaneous (MSC)
- Rec. 50. Android (DRD)

Secure Java Coding Books

There are two books available that cover Java: one for rules and the other for guidelines.

- Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs provides guidelines, recommendations, and examples to enable the creation of reliable, robust, fast, maintainable, and secure code.

Source Code Analysis Laboratory (SCALe)

SCALe offers conformance testing of Java language software systems against the CERT Oracle Secure Coding Standard for Java.

Contact Us

Contact us if you
- have questions about the Secure Coding wiki
- have recommendations for standards in development
- want to request privileges to participate in standards development

Thank You!

We acknowledge the contributions of the following folks, and we look forward to seeing your name here as well.
Rules vs. Recommendations
This coding standard consists of rules and recommendations, collectively referred to as guidelines. Rules are meant to provide normative requirements for code, whereas recommendations are meant to provide guidance that, when followed, should improve the safety, reliability, and security of software systems. Learn more about the differences.

Linking to Our Pages
Link to guidelines using the Tiny Link under ToolsLink to this Page... (This URL will not change if the name of the guideline changes.)

Information for Editors
- To eliminate a section from the lists above, label it section and void.
- To have a section listed as a recommendation, label it section and recommendation.
- To have a section listed as a rule, label it section and rule.