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.

Front Matter

Rules

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

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. 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. 15. Platform Security (SEC)
- Rec. 18. Concurrency (CON)
- Rec. 49. Miscellaneous (MSC)

Content by label

There is no content with the specified labels.
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.