Rule 15. Platform Security (SEC)

Rules

- SEC00-J. Do not allow privileged blocks to leak sensitive information across a trust boundary
- SEC01-J. Do not allow tainted variables in privileged blocks
- SEC02-J. Do not base security checks on untrusted sources
- SEC03-J. Do not load trusted classes after allowing untrusted code to load arbitrary classes
- SEC04-J. Protect sensitive operations with security manager checks
- SEC05-J. Do not use reflection to increase accessibility of classes, methods, or fields
- SEC06-J. Do not rely on the default automatic signature verification provided by URLClassLoader and java.util.jar
- SEC07-J. Call the superclass's getPermissions() method when writing a custom class loader
- SEC08-J Trusted code must discard or clean any arguments provided by untrusted code
- SEC09-J Never leak the results of certain standard API methods from trusted code to untrusted code
- SEC10-J Never permit untrusted code to invoke any API that may (possibly transitively) invoke the reflection APIs

Risk Assessment Summary

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
SEC00-J	Medium	Likely	High	P6	L2
SEC01-J	High	Likely	Low	P27	L1
SEC02-J	High	Probable	Medium	P12	L1
SEC03-J	High	Probable	Medium	P12	L1
SEC04-J	High	Probable	Medium	P12	L1
SEC05-J	High	Probable	Medium	P12	L1
SEC06-J	High	Probable	Medium	P12	L1
SEC07-J	High	Probable	Low	P18	L1