Java analysis 1.20

Analysis in all applications

The following changes in version 1.20 affect Java analysis in all applications.

General improvements

The `FlowSources` and `TaintTracking` libraries are extended to cover additional remote user input and taint steps from the following frameworks: Guice, Protobuf, Thrift and Struts. This affects all security queries, which may yield additional results on projects that use these frameworks.

New queries

Query	Tags	Purpose
Double-checked locking is not thread-safe (`java/unsafe-double-checked-locking`)	reliability, correctness, concurrency, external/cwe/cwe-609	Identifies wrong implementations of double-checked locking that does not use the `volatile` keyword.
Race condition in double-checked locking object initialization (`java/unsafe-double-checked-locking-init-order`)	reliability, correctness, concurrency, external/cwe/cwe-609	Identifies wrong implementations of double-checked locking that performs additional initialization after exposing the constructed object.

Changes to existing queries

Query	Expected impact	Change
Arbitrary file write during archive extraction (“Zip Slip”) (`java/zipslip`)	Fewer false positive results	Results involving a sanitization step that converts a destination `Path` to a `File` are no longer reported.
Result of multiplication cast to wider type (`java/integer-multiplication-cast-to-long`)	Fewer results	Results involving conversions to `float` or `double` are no longer reported, as they were almost exclusively false positives.

Changes to QL libraries

- The deprecated library `semmle.code.java.security.DataFlow` has been removed. Improved data flow libraries have been available in `semmle.code.java.dataflow.DataFlow`, `semmle.code.java.dataflow.TaintTracking`, and `semmle.code.java.dataflow.FlowSources` since 1.16.

- Taint tracking now includes additional default data-flow steps through collections, maps, and iterators. This affects all security queries, which can report more results based on such paths.

Additional changes for analysis in QL tools and applications only

There are no changes in this version that affect Java analysis only in QL for Eclipse, and the QL command-line tools.