UNCHECKED\_FUNC\_RES.STAT

Детектор указывает на случаи, когда результат функции не проверяется, при этом используется статистический подход: если в большинстве аналогичных вызовов результат проверяется, то и в данном месте рекомендуется это сделать.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | Normal |
| Надежность | High |
| Источник | SvEng |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE252;CWE754 |
| CVE | — |
| Возможные последствия | Игнорирование результата может привести к ошибкам выполнения, особенно если функция сигнализирует о сбоях через возвращаемое значение. |
| Комментарий | Даже если явных признаков ошибки нет, статистически значимые отклонения от общей практики могут указывать на потенциальные уязвимости или недоработки. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest(String s) {  // результат не защищён, может упасть  int value = Integer.parseInt(s);  System.out.println("Parsed: " + value);  } | public static void correctTest(String s) {  try {  int value = Integer.parseInt(s);  System.out.println("Parsed: " + value);  } catch (NumberFormatException e) {  System.out.println("Invalid number!");  }  } |