INT\_OVERFLOW.LIB

Обычно возникает, когда результат арифметической операции превышает максимальное или минимальное допустимое значение для типа int, вызванное библиотечной функцией.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | Normal |
| Надежность | Average |
| Источник | SvEng |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE190;CWE191;CWE194;CWE195;CWE196;CWE197 |
| CVE | — |
| Возможные последствия | Использование библиотечных функций, которые могут вызвать переполнение, может привести к неожиданным результатам, сбоям в работе программы или уязвимостям, если переполнение не обработано должным образом. |
| Комментарий | Важно внимательно следить за вызовами библиотечных функций, которые могут неявно вызывать переполнение, особенно при работе с числами, близкими к пределам типа данных. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest(int a, int b) {  // Math.addExact выбрасывает исключение при переполнении  int result = Math.addExact(a, b);  System.out.println("Result: " + result);  } | public static void correctTest(int a, int b) {  if (a > Integer.MAX\_VALUE - b) {  System.out.println("Overflow would occur!");  } else {  int result = a + b;  System.out.println("Result: " + result);  }  } |

Методы устранения уязвимости при срабатывании детектора:

1. Внимательно изучите документацию библиотечной функции, чтобы понять, как она обрабатывает переполнение. Некоторые функции могут возвращать специальные значения (например, обрезать результат), другие могут выбрасывать исключения (ArithmeticException в случае Math.addExact() и подобных в Java), а третьи могут не иметь явной обработки переполнения.
2. Если библиотечная функция выбрасывает исключение при переполнении, оберните вызов этой функции в блок try-catch и обработайте исключение соответствующим образом. Это может включать логирование ошибки, возврат специального значения, выполнение альтернативных действий или выброс собственного исключения.