INT\_OVERFLOW.AFTER\_CHECK

В статическом анализаторе Svace, предупреждение OVERFLOW\_AFTER\_CHECK указывает на ситуацию, когда происходит переполнение (overflow) после проверки на переполнение. Это означает, что в коде есть проверка на переполнение (например, проверка, не превышает ли значение некоторого числа максимально допустимое значение), но после этой проверки все равно происходит операция, которая может вызвать переполнение.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | Normal |
| Надежность | Low |
| Источник | SvEng |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE190;CWE191;CWE194;CWE195;CWE196;CWE197 |
| CVE | — |
| Возможные последствия | Может привести к неверным вычислениям, логическим ошибкам и уязвимостям безопасности, несмотря на наличие на первый взгляд корректной защиты. |
| Комментарий | Необходимо удостовериться, что операция, способная вызвать переполнение, действительно защищена соответствующей проверкой, и что между проверкой и операцией не происходит изменения переменных. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest(int a, int b) {  if (a < Integer.MAX\_VALUE) {  int result = a \* b; // переполнение здесь  System.out.println("Результат (переполнен): " + result);  }  } | public static void correctTest(int a, int b) {  long temp = (long) a \* b;  if (temp <= Integer.MAX\_VALUE) {  int result = (int) temp;  System.out.println("Результат: " + result);  } else {  System.out.println("Переполнение при умножении!");  }  } |

Методы устранения уязвимости при срабатывании детектора:

1. Убедитесь, что операция, которая может вызвать переполнение, выполняется только в том случае, если проверка гарантирует отсутствие переполнения. Проверьте логику условия if.
2. Используйте более широкий тип данных (например, long вместо int) для выполнения потенциально переполняющейся операции. Затем, если результат находится в пределах допустимого диапазона исходного типа, приведите его обратно.
3. Перенесите проверку на переполнение непосредственно перед опасной операцией. Убедитесь, что между проверкой и операцией не происходит изменений переменных, которые могут привести к переполнению.