INT\_OVERFLOW.SHIFT

Предупреждение указывает на ситуацию, когда происходит переполнение целого числа в результате операции сдвига.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | Normal |
| Надежность | VeryLow |
| Источник | SvEng |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE190;CWE191;CWE194;CWE195;CWE196;CWE197 |
| CVE | — |
| Возможные последствия | Переполнение при сдвиге может привести к потере данных или непредсказуемому поведению программы, особенно если сдвиг выполняется на слишком большие значения. |
| Комментарий | При использовании операций сдвига следует удостовериться, что количество позиций для сдвига не превышает допустимый диапазон, чтобы избежать переполнения. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest(int a) {  int result = a << 1;  System.out.println("Result: " + result);  } | public static void correctTest(int a) {  if (a > Integer.MAX\_VALUE >> 1) {  System.out.println("Overflow would occur if shifted!");  } else {  int result = a << 1;  System.out.println("Result: " + result);  }  } |

Методы устранения уязвимости при срабатывании детектора:

1. Перед выполнением операции сдвига влево (<<) проверьте, не приведет ли сдвиг к выходу за пределы диапазона типа int. Для сдвига на n бит влево, значение a не должно превышать Integer.MAX\_VALUE >> n (для положительных a).
2. Используйте тип данных с большим диапазоном (long) для выполнения операции сдвига, если результат может превысить Integer.MAX\_VALUE или быть меньше Integer.MIN\_VALUE. Затем, при необходимости, приведите результат обратно к int, предварительно убедившись, что он находится в допустимом диапазоне.
3. Убедитесь, что количество битов для сдвига не является отрицательным и не превышает или равно количеству битов в типе данных (32 для int). Сдвиг на 32 или более бит для int приводит к неопределенному поведению (в Java результат сдвига s вычисляется как s & 0x1f).