FB.IM\_AVERAGE\_COMPUTATION\_COULD\_OVERFLOW

Детектор определяет ошибку, в ходе которой код вычисляет среднее значение двух целых чисел, используя либо деление, либо сдвиг вправо со знаком, а затем использует результат в качестве индекса массива. Если усредняемые значения очень велики, это может привести к переполнению (что приведет к вычислению отрицательного среднего). Предполагая, что результат должен быть неотрицательным, вместо этого вы можете использовать беззнаковый сдвиг вправо. Другими словами, вместо использования (низкий+высокий)/2 используйте (низкий+высокий) >>> 1.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Ошибка разработчика |
| CWE | — |
| CVE | — |
| Возможные последствия | При вычислении среднего двух больших целых чисел (например, low + high) может произойти переполнение, что приведет к отрицательному значению индекса массива и потенциальному ArrayIndexOutOfBoundsException. |
| Комментарий | Чтобы избежать переполнения, используйте беззнаковый сдвиг вправо (>>> 1) вместо деления. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest() {  int low = Integer.MAX\_VALUE - 1;  int high = Integer.MAX\_VALUE;    // может привести к переполнению  int mid = (low + high) / 2;  System.out.println("Incorrect mid: " + mid);  } | public static void correctTest() {  int low = Integer.MAX\_VALUE - 1;  int high = Integer.MAX\_VALUE;  // предотвращает переполнение  int mid = (low + high) >>> 1;  System.out.println("Correct mid: " + mid);  } |

Методы устранения уязвимости при срабатывании детектора:

1. **Замените (low + high) / 2 на (low + high) >>> 1:** При вычислении среднего значения двух целых чисел, которые могут быть большими, используйте оператор беззнакового сдвига вправо. Это предотвращает переполнение, так как сложение выполняется в обычном режиме, но затем результат интерпретируется как беззнаковое число перед сдвигом, эффективно деля его на 2 без риска получения отрицательного результата.
2. **Проверьте все места вычисления среднего:** Найдите в коде все случаи вычисления среднего двух целых чисел, особенно если результат используется в качестве индекса массива или в других контекстах, где ожидается неотрицательное значение.
3. **Убедитесь в неотрицательности границ:** Если известно, что границы (low и high) всегда неотрицательны, использование беззнакового сдвига все равно является более безопасным подходом.
4. **Рассмотрите альтернативные способы вычисления среднего:** В некоторых случаях можно использовать формулу low + (high - low) / 2, которая также позволяет избежать переполнения, но беззнаковый сдвиг часто является более лаконичным и эффективным.