FB.BIT\_SIGNED\_CHECK\_HIGH\_BIT

Этот метод сравнивает побитовое выражение, такое как ((val & CONSTANT) > 0), где CONSTANT - отрицательное число. Использование битовой арифметики и последующее сравнение с оператором "больше, чем" может привести к неожиданным результатам. Это сравнение вряд ли сработает должным образом. Хорошей практикой является использование '!= 0' вместо '> 0'.

Таблица №1 – Основные характеристики детектора FB.BIT\_SIGNED\_CHECK\_HIGH\_BIT

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Некорректная проверка знакового бита (Signed Bit Check Error) |
| CWE | --- |
| CVE | --- |
| Возможные последствия | * Неправильная обработка отрицательных чисел * Логические ошибки в условиях * Уязвимости в криптографических или битовых операциях |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  int value = -42;  if ((value & 0x80) != 0) { // ОШИБКА: проверка только 8-го бита, а не знакового  System.out.println("Negative number detected (INCORRECT)");  } else {  System.out.println("Positive number (INCORRECT)");  }  } | public static void correctTest() {  int value = -42;  if (value < 0) { // Правильный способ проверки знака  System.out.println("Negative number detected (CORRECT)");  } else {  System.out.println("Positive number (CORRECT)");  }  } |