* + 1. FB.INT\_BAD\_COMPARISON\_WITH\_SIGNED\_BYTE

Детектор определяет ошибку, в ходе которой байты со знаком могут иметь значение только в диапазоне от -128 до 127. Сравнение байта со знаком со значением вне этого диапазона бессмысленно и, вероятно, будет неверным. Чтобы преобразовать знаковый байт b в беззнаковое значение в диапазоне 0..255, используйте 0xff & b.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | UAST |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE-190 (Integer Overflow or Wraparound), CWE-682 (Incorrect Calculation) |
| CVE | — |
| Возможные последствия | Некорректные результаты сравнения, логические ошибки в коде, потенциальные уязвимости, связанные с неправильной интерпретацией знакового байта |
| Комментарий | Сравнение byte со значением за пределами -128..127 бессмысленно и может приводить к ошибкам. Для корректного сравнения с числами от 0 до 255 следует использовать 0xff & b для приведения к беззнаковому int. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest() {  byte value = 100;  if (value > 128) {  // ...  }  } | public static void correctTest() {  byte value = 100;  // Преобразование в беззнаковый int  int unsignedValue = value & 0xff;  if (unsignedValue > 128) {  // ...  }  } |