FB.BC\_VACUOUS\_INSTANCEOF

Детектор определяет ошибку, в ходе которой тест экземпляра всегда будет возвращать значение true (если только проверяемое значение не равно нулю). Хотя это и безопасно, убедитесь, что это не является признаком какого-то недопонимания или какой-либо другой логической ошибки. Если вы действительно хотите проверить значение на нулевое значение, возможно, было бы яснее выполнить нулевую проверку, а не проверку экземпляра.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE571 |
| CVE | — |
| Возможные последствия | Использование instanceof, которое всегда возвращает true, может указывать на логическую ошибку или избыточную проверку, не имеющую практической пользы. |
| Комментарий | Проверьте, действительно ли проверка instanceof необходима. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest() {  class MyClass {  void checkInstance(Object obj) {  // всегда истинна, если obj не null  if (obj instanceof Object) {  System.out.println("...");  }  }  }  MyClass myClass = new MyClass();  myClass.checkInstance(new String("Hello"));  myClass.checkInstance(null); // null не пройдет проверку  } | public static void correctTest() {  class MyClass {  void checkInstance(Object obj) {  // явная проверка на null  if (obj != null) {  System.out.println("obj не равен null");  }  }  }  MyClass myClass = new MyClass();  myClass.checkInstance(new String("Hello"));  myClass.checkInstance(null);  } |

Методы устранения уязвимости при срабатывании детектора:

1. **Замените на проверку на null:** Если целью проверки было исключить null, замените obj instanceof Object (или аналогичную всегда истинную проверку instanceof) на явную проверку obj != null.
2. **Пересмотрите логику:** Убедитесь, что вы действительно понимаете, почему используется instanceof. Возможно, вы пытались проверить более конкретный тип, и произошла ошибка. Исправьте тип для проверки.
3. **Удалите избыточную проверку:** Если проверка instanceof с базовым типом (Object) не несет никакой дополнительной информации (кроме проверки на null), рассмотрите возможность ее удаления, если проверка на null уже выполняется в другом месте или не требуется.
4. **Сделайте код более явным:** Даже если проверка instanceof с базовым типом кажется логически верной в контексте, рассмотрите возможность сделать код более читаемым, явно выразив намерение (например, через проверку на null).