FB.REC\_CATCH\_EXCEPTION

Детектор определяет ошибку, в ходе которой метод использует блок try-catch, который перехватывает объекты Exception, но Exception не генерируется внутри блока try, а RuntimeException не перехватывается явным образом. Распространенной ошибкой является выражение try { ... } catch (Exception e) { Something } как сокращение для перехвата нескольких типов исключений, каждый из блоков catch которых идентичен, но эта конструкция также случайно перехватывает RuntimeException. , маскируя потенциальные ошибки.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Ошибка разработчика |
| CWE | CWE396 |
| CVE | — |
| Возможные последствия | Перехват Exception без необходимости может скрыть ошибки, включая RuntimeException, что затруднит отладку и выявление критических проблем. |
| Комментарий | Следует перехватывать только конкретные исключения, которые действительно могут возникнуть в блоке try, и отдельно обрабатывать RuntimeException, если это необходимо. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest() {  try {  System.out.println("код не выбрасывает Exception");  } catch (Exception e) {  System.out.println("Перехват Exception, но внутри try нет его источника");  }  } | public static void correctTest() {  try {  throw new IllegalArgumentException("Пример RuntimeException");  } catch (IllegalArgumentException e) {  System.out.println("Перехвачена IllegalArgumentException: " + e.getMessage());  }  } |