FB.MS\_MUTABLE\_HASHTABLE

Последнее статическое поле ссылается на хэш-таблицу, к которой можно получить доступ с помощью вредоносного кода или случайно, через другой пакет. Этот код может свободно изменять содержимое Hashtable.

Таблица №1 – Основные характеристики детектора FB.MS\_MUTABLE\_HASHTABLE

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Data Integrity Vulnerability |
| CWE | CWE-218 |
| CVE | --- |
| Возможные последствия | Потеря данных: изменение ключа после вставки делает элемент недоступным для поиска/удаления; утечка памяти: накопление "потерянных" записей в хэш-таблице из-за невозможности доступа; DoS-атаки: возможность преднамеренного создания коллизий для замедления работы системы |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  Hashtable<MutableKey, String> table = new Hashtable<>();  MutableKey key = new MutableKey("ID1");  table.put(key, "Confidential Data");    // Изменение ключа после вставки  key.setValue("MODIFIED\_ID");  System.out.println("Поиск по измененному ключу: " + table.get(key)); // null  } | public static void correctTest() {  Hashtable<ImmutableKey, String> table = new Hashtable<>();  ImmutableKey key = new ImmutableKey("ID1");  table.put(key, "Secure Data");    // Попытка изменения ключа невозможна (компиляция запрещена)  System.out.println("Корректный поиск: " + table.get(key)); // Secure Data  } |