FB.DM\_CONVERT\_CASE

Строка преобразуется в верхний или нижний регистр с использованием кодировки платформы по умолчанию. Это может привести к неправильным преобразованиям при использовании международных символов. Вместо этого следует использовать String.toUpperCase( Locale l ), String.toLowerCase( Locale l ).

Таблица №1 – Основные характеристики детектора FB.DM\_CONVERT\_CASE

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Case Conversion Locale Vulnerability |
| CWE | --- |
| CVE | --- |
| Возможные последствия | Некорректное сравнение строк в локале-зависимых операциях; нарушение бизнес-логики при проверке чувствительных к регистру данных; проблемы безопасности при валидации строк (например, паролей, токенов); несовместимость между системами с разными локалями. |
| Комментарий | Ошибка возникает при использовании String.toUpperCase()/toLowerCase() без указания локали, локаль-зависимых операций в критически важных проверках, преобразований для нормализации строк сравнения. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // 1. Локаль-зависимое преобразование  String input = "i";  String upper = input.toUpperCase(); // В турецкой локале станет "İ" (U+0130)    // 2. Ненадёжное сравнение  if ("MAIL".equals(input.toUpperCase())) { // Зависит от системной локали  System.out.println("Match found");  }  // 3. Преобразование для хранения  String normalized = "ß".toLowerCase(); // В немецкой локале станет "ss"  System.out.println(normalized);  } | public static void correctTest() {  // 1. Явное указание локали  String input = "i";  String upper = input.toUpperCase(Locale.ENGLISH); // Всегда "I"  // 2. Надёжное сравнение  if ("MAIL".equalsIgnoreCase(input)) { // Или:  // if ("MAIL".equals(input.toUpperCase(Locale.ROOT))) {  System.out.println("Reliable match");  }  // 3. Контролируемая нормализация  String normalized = "ß".toLowerCase(Locale.GERMAN); // Явное преобразование  System.out.println("Normalized: " + normalized);  } |

Методы устранения уязвимости при срабатывании детектора.

1. Явное указание локали;
2. Использование Locale.ROOT для машинно-ориентированных строк;
3. equalsIgnoreCase() для простых сравнений;
4. Нормализация перед сравнением.