FB.MS\_SHOULD\_BE\_REFACTORED\_TO\_BE\_FINAL

Это общедоступное статическое или защищенное статическое поле не является окончательным и может быть изменено вредоносным кодом или случайно из другого пакета. Чтобы избежать этой уязвимости, поле лучше сделать окончательным. Однако статический инициализатор содержит более одной записи в поле, поэтому для этого потребуется некоторый рефакторинг.

Таблица №1 – Основные характеристики детектора FB.MS\_SHOULD\_BE\_REFACTORED\_TO\_BE\_FINAL

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability (Mutable Static Field) |
| CWE | CWE218 |
| CVE | --- |
| Возможные последствия | Непреднамеренное изменение статического поля, приводящее к неожиданному поведению программы; возможность атак, если поле содержит конфиденциальные данные; нарушение потокобезопасности в многопоточной среде. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Вредоносный код может изменить список привилегированных пользователей  ConfigurationIncorrect.PRIVILEGED\_USERS.add("hacker");  System.out.println("Incorrect users: " + ConfigurationIncorrect.PRIVILEGED\_USERS);  } | public static void correctTest() {  // Попытка изменения приведет к UnsupportedOperationException  try {  ConfigurationCorrect.getPrivilegedUsers().add("hacker");  } catch (UnsupportedOperationException e) {  System.out.println("Correct behavior: " + e.getMessage());  }  System.out.println("Correct users: " + ConfigurationCorrect.getPrivilegedUsers());  } |