FB.MS\_FINAL\_PKGPROTECT

Изменяемое статическое поле может быть изменено вредоносным кодом или случайно из другого пакета. Поле можно сделать защищенным пакетом и/или сделать окончательным, чтобы избежать этой уязвимости.

Таблица №1 – Основные характеристики детектора FB.MS\_FINAL\_PKGPROTECT

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Уязвимость контроля доступа к данным (Data Access Control Vulnerability) |
| CWE | CWE-218 |
| CVE | --- |
| Возможные последствия | Несанкционированное изменение важных статических данных приложения; нарушение логики работы программы и целостности данных; возможность внедрения вредоносного кода через модификацию статических полей; непредсказуемое поведение приложения из-за неконтролируемых изменений состояния; компрометация безопасности приложения при изменении чувствительных данных (URL-адресов, ключей API и т.д.) |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void correctTest() {  // Доступ к безопасному финальному полю (его нельзя изменить)  System.out.println("Безопасный API\_KEY (final): " + SecureConfiguration.API\_KEY);    // Следующая строка вызвала бы ошибку компиляции:  // SecureConfiguration.API\_KEY = "compromised\_key\_12345"; // Ошибка компиляции    // Доступ к защищенному пакетному полю возможен только внутри пакета  SecureConfiguration.defaultTimeout = 30;  System.out.println("Пакетно-защищенное поле: " + SecureConfiguration.defaultTimeout);  } | public static void incorrectTest() {  // Уязвимое статическое поле может быть изменено из любого места  System.out.println("Исходное значение API\_KEY: " + VulnerableConfiguration.API\_KEY);    // Имитация изменения из другого пакета (потенциально вредоносного)  VulnerableConfiguration.API\_KEY = "compromised\_key\_12345";  System.out.println("Измененное значение API\_KEY: " + VulnerableConfiguration.API\_KEY);    // Это может привести к компрометации безопасности приложения  } |