FB.MS\_OOI\_PKGPROTECT

Последнее статическое поле, определенное в интерфейсе, ссылается на изменяемый объект, например массив или хеш-таблицу. Этот изменяемый объект может быть изменен вредоносным кодом или случайно из другого пакета. Чтобы решить эту проблему, поле необходимо переместить в класс и сделать пакет защищенным, чтобы избежать эту уязвимость.

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

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability (Insecure Object Exposure) |
| CWE | CWE218 |
| CVE | --- |
| Возможные последствия | Несанкционированная модификация изменяемого объекта (например, массива или коллекции) из другого пакета; нарушение инкапсуляции, приводящее к неожиданным изменениям состояния программы; возможность атак, связанных с подменой данных. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Вредоносный код может изменить массив напрямую  DataHolderIncorrect.sensitiveArray[0] = "hacked!";  } | public static void correctTest() {  // Получаем защищённую копию, оригинал остаётся неизменным  String[] copy = DataHolderCorrect.getSensitiveArray();  copy[0] = "attempted\_hack"; // Не влияет на исходный массив  } |