FB.XFB\_XML\_FACTORY\_BYPASS

Этот метод выделяет конкретную реализацию интерфейса XML. Предпочтительнее использовать предоставленные фабричные классы для создания этих объектов, чтобы можно было изменить реализацию во время выполнения.

Таблица №1 – Основные характеристики детектора FB.XFB\_XML\_FACTORY\_BYPASS

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability |
| CWE | --- |
| CVE | --- |
| Возможные последствия | * XXE (XML External Entity) атаки * Доступ к локальным файлам системы * SSRF (Server Side Request Forgery) |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Некорректно: уязвимая конфигурация XML парсера  try {  DocumentBuilderFactory factory = DocumentBuilderFactory.newInstance();  DocumentBuilder builder = factory.newDocumentBuilder();  Document doc = builder.parse("input.xml"); // Уязвимость!  System.out.println("XML parsed (INSECURE)");  } catch (Exception e) {  e.printStackTrace();  }  } | public static void correctTest() {  // Корректно: безопасная конфигурация XML парсера  try {  DocumentBuilderFactory factory = DocumentBuilderFactory.newInstance();  factory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true);  factory.setFeature("http://xml.org/sax/features/external-general-entities", false);  factory.setFeature("http://xml.org/sax/features/external-parameter-entities", false);  factory.setXIncludeAware(false);  factory.setExpandEntityReferences(false);    DocumentBuilder builder = factory.newDocumentBuilder();  Document doc = builder.parse("input.xml");  System.out.println("XML parsed securely");  } catch (Exception e) {  e.printStackTrace();  }  } |