FB.DMI\_CONSTANT\_DB\_PASSWORD

Этот код создает соединение с базой данных с использованием строго записанного в коде постоянного пароля. Любой, у кого есть доступ к исходному или скомпилированному коду, может легко узнать пароль.

Таблица №1 – Основные характеристики детектора FB.DMI\_CONSTANT\_DB\_PASSWORD

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability |
| CWE | CWE259 |
| CVE | --- |
| Возможные последствия | Возможность несанкционированного доступа к базе данных; утечка конфиденциальных данных; нарушение политик безопасности предприятия; юридические последствия при утечке данных |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Некорректно: пароль в открытом виде в коде  try {  Connection conn = DriverManager.getConnection(  "jdbc:mysql://localhost:3306/mydb",  "admin",  "SuperSecret123!"); // Пароль в коде  System.out.println("Connected (INSECURE)");  conn.close();  } catch (SQLException e) {  e.printStackTrace();  }  } | public static void correctTest() {  // Корректно: получение учетных данных из защищенного источника  try {  String password = System.getenv("DB\_PASSWORD"); // Из переменных окружения  Connection conn = DriverManager.getConnection(  "jdbc:mysql://localhost:3306/mydb",  "admin",  password);  System.out.println("Connected (SECURE)");  conn.close();  } catch (SQLException e) {  e.printStackTrace();  }  } |