FB.DP\_CREATE\_CLASSLOADER\_INSIDE\_DO\_PRIVILEGED

Детектор определяет ошибку, в ходе которой код создает загрузчик классов, которому требуется разрешение, если установлено управление безопасностью. Если этот код может быть вызван кодом, не имеющим разрешений безопасности, то создание загрузчика классов должно происходить внутри блока doPrivileged.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Ошибка разработчика |
| CWE | — |
| CVE | — |
| Возможные последствия | Создание загрузчика классов без использования блока doPrivileged может привести к сбоям безопасности, если код выполняется в окружении с ограниченными правами. Это может привести к исключениям, связанным с безопасностью, или невозможности загрузить необходимые классы. |
| Комментарий | Если создание загрузчика классов требует привилегий безопасности, следует поместить его в блок doPrivileged, чтобы обеспечить корректное выполнение в средах с ограниченными правами доступа. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public void incorrectTest() {  // без использования doPrivileged  ClassLoader classLoader = this.getClass().getClassLoader();  // ...  } | public void correctTest() {  // внутри блока doPrivileged  ClassLoader classLoader = AccessController.doPrivileged(new PrivilegedAction<ClassLoader>() {  @Override  public ClassLoader run() {  return this.getClass().getClassLoader();  }  });  // ...  } |

Методы устранения уязвимости при срабатывании детектора:

1. **Оберните создание ClassLoader в doPrivileged:** Код, который непосредственно создает экземпляр ClassLoader (или его подкласса), должен быть выполнен внутри блока AccessController.doPrivileged.
2. **Используйте PrivilegedAction или PrivilegedExceptionAction:** Передайте экземпляр PrivilegedAction (если операция не бросает проверяемых исключений) или PrivilegedExceptionAction (если операция может бросать проверяемые исключения) в метод doPrivileged. В методе run() этого действия выполняйте создание загрузчика классов.
3. **Проверьте требования безопасности:** Убедитесь, что создание конкретного типа загрузчика классов действительно требует привилегий безопасности в вашем окружении с активным менеджером безопасности.
4. **Рассмотрите альтернативы:** В некоторых случаях может быть возможно избежать создания кастомного загрузчика классов, используя существующие механизмы загрузки или решая проблему другим способом, не требующим специальных привилегий.
5. **Будьте внимательны к контексту вызова:** Если ваш код может быть вызван кодом с ограниченными правами, обеспечение работы с привилегиями через doPrivileged становится критически важным для безопасности и корректной работы.