Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | My MTS |
| Версия | | 2.4.7 |
| Дата проверки | | 04.03.2019 |
| Проверил | | Томашевич Константин |
| Конфиденциальная информация | |  |
| **Требования безопасности** | | **Результат** |
| 1 | Ненадежное хранение данных | - |
| 1.1 | Локальное хранение конфиденциальных данных  STORAGE-1 и STORAGE-2 | - |
| 1.1.1 | наличие разрешений AndroidManifest.xml для read/write во внешнем хранилище | Есть разрешения на чтение/запись в external storage. Я поискал файлы приложения на external storage и однозначно приложению принадлежит только кэш `MapKit`. Поэтому скорее всего ничего конфиденциального они в external storage не хранят. |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | Все SharedPreferences открываются с MODE\_PRIVATE. Есть один вызов getDir с MODE\_PRIVATE. Не нашёл других методов, которые могли бы использовать MODE\_WORLD\_\*. |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | **SharedPreferences**  Используются в LocalStorage, ModelStorage, WidgetStorage.  В LocalStorage, по моим наблюдением, хранятся куки. При этом все изменения и запросы значений LocalStorage записываются в дебажный лог, что фактически делает настройки из LocalStorage равнозначными MODE\_WORLD\_READABLE настройкам. Пока не установил хранится ли там что-то действительно важное, но есть подозрения что там проскакивает как минимум телефонный номер пользователя.  WidgetStorage льёт многие изменения из SharedPreferences в ReportUtil, который льёт всё в YandexMetrica. Пока не установил важность информации и можно ли её перехватить из метрики яндекса.  **FileOutputStream**  Используется в WidgetStorage и StepsFragment для сохранения каких иконок. В том числе есть сохранение на external storage, но оно скорее всего инициируется именно пользователем, так как метод зовётся share.  **FileInputStream**  WidgetStorage грузит какие-то иконки, но они находятся во внутренней папке, открытой с помощью getDir с MODE\_PRIVATE.  **getExternal\***  StepsFragment использует getExternalFilesDir(Environment.DIRECTORY\_PICTURES) в методе share. Исходя из контекста это сохранение чего-либо пользователем, поэтому уязвимостью не является.  **getWritableDatabase**  Не нашёл использований.  **getReadableDatabase**  Не нашёл использований.  **getCacheDir**  Не нашёл использований.  **getExternalCacheDirs**  Не нашёл использований. |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | Нашёл кучу \*.properties файлов, но там только версии плагинов.  В манифесте нашёл такую интересную строку:  <meta-data android:name="io.fabric.ApiKey" android:value="94284c61ee7949c560f549ff5f7b374dd7c68371"/>  В MainActivity.java есть ещё такой интересный кусок кода:  MapKitFactory.setApiKey("0def7909-cf07-4c07-ad55-206c6821f5e0"); |
| 1.1.5 | файлы ресурсов | Нашёл ключ для работы с API Yandex: 8784accb-db3e-4026-bc75-dc2909ad90e1.  Нашёл ключ для работы с API Google: AIzaSyD\_swstDa1E57iRhcvDdZOwfxxwYBipX1Y.  Нашёл ключ для работы с Google Crash Reporting API: AIzaSyD\_swstDa1E57iRhcvDdZOwfxxwYBipX1Y.  Очень интересно выглядит ключ для API Google Maps, представляю полную строку из файла: <string name="google\_maps\_key">YOUR\_KEY\_HERE</string>.  Нашёл идентификатор сборки для Crashlytics (не знаю, насколько это важно): 286fcdfc-031c-4e6a-a74b-858cbf8a6f15.  Нашёл Google App Id: 1:255084819593:android:ff3f4088b8315f9a.  Пока не знаю, для чего эти строки, но выглядят они интересно:  <string name="path\_password\_eye">M12,4.5C7,4.5 2.73,7.61 1,12c1.73,4.39 6,7.5 11,7.5s9.27,-3.11 11,-7.5c-1.73,-4.39 -6,-7.5 -11,-7.5zM12,17c-2.76,0 -5,-2.24 -5,-5s2.24,-5 5,-5 5,2.24 5,5 -2.24,5 -5,5zM12,9c-1.66,0 -3,1.34 -3,3s1.34,3 3,3 3,-1.34 3,-3 -1.34,-3 -3,-3z</string>  <string name="path\_password\_eye\_mask\_strike\_through">M2,4.27 L19.73,22 L22.27,19.46 L4.54,1.73 L4.54,1 L23,1 L23,23 L1,23 L1,4.27 Z</string>  <string name="path\_password\_eye\_mask\_visible">M2,4.27 L2,4.27 L4.54,1.73 L4.54,1.73 L4.54,1 L23,1 L23,23 L1,23 L1,4.27 Z</string>  <string name="path\_password\_strike\_through">M3.27,4.27 L19.74,20.74</string> |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | ActionManager.getData печает в лог всё что делает. Пока не проверил, есть ли там что-то важное.  Все вызовы Logix.getCookie летят в лог вместе с ключами и значениями. Пока не проверил, есть ли там что-то важное. Также куки хранятся в LocalStorage. В ScreenManager.java#L163 ищется значение кука phone, пока что не получилось проверить действительно ли это номер телефона пользователя.  Очень много других вызовов логинга (479+ только для дебажных сообщений), пока что не разбирал вылетает ли через них что-то потенциально конфиденциальное. |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 |  |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 |  |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 |  |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 |  |
| 1.7 | Резервное копирование STORAGE-8 |  |
| 1.8 | … |  |
|  |  |  |