Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | Spotify |
| Версия | | 8.4.74.463 |
| Дата проверки | | 04.03.2020 |
| Проверил | | Желтовский Кирилл |
| Конфиденциальная информация | | Любимые песни, альбомы, плейлисты, предпочтения, логин, пароль, доступ к контактам |
| **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 | C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_19-32-19.png  имеются |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | Данные доступ к файлам не осуществляется |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | SharedPreferences активно используются. C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_19-58-15.png  Использование FileOutputStream также встречается  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_19-59-29.png  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_20-00-12.png  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_20-00-53.png  Вызовы getWritableDatabase и getReadableDatabase нашлись только в неправильно декомпилированном коде.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-04_20-03-05.png  Вызовов getExternalCacheDirs не нашлось. |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | Доступ к данным файлам получить не удалось, так как в распоряжении имелся лишь apk файл |
| 1.1.5 | файлы ресурсов | Файл строковых ресурсов состоит из 2275 строк. Ничего подозрительного по поиску слов pass, password, key найдено не было. |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | Разработчики данного приложения не использовали пакет android.util.Log, в исходном коде встречается собственный класс Logger. Причём его код обфусцирован, что затрудняет попытки разобраться, что происходит внутри. Пробежавшись по нахождения использования данного логгера, подозрительных использований найдено не было, причем случаи с динамическим конструированием строки в качестве параметра тоже не были найдены.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_16-51-39.png  Папка в data/data:  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_21-52-55.png |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 | Среди используемых библиотек выделяются Retrofit для работы со сторонними API, Crashlytics для отслеживания проблем с приложением, Picasso для загрузки изображений и другие.  Retrofit используется для взаимодействия с серверами, например, для получения информации о музыканте, плейлистах, что в общем-то не представляет никакой опасности для пользователя.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_22-34-08.png  Также происходит взаимодействие с сервисом настройки конфигурации, куда приложение передаёт X-installation-id  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_22-36-04.png  Имеется интерфейс для взаимодействия с сервисом входа в приложения, куда передается информация о почте/фейсбуке.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_22-37-20.png  Данная информация передаётся скорее всего на сервисы разработчиков приложения, что делается с ними в дальнейшем непонятно. |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 | При вводе пароля на экране входа, кеш клавиатуры не появляется, скриншот, свидетельствующий об этом, сделать не получается, а всплывает уведомление, говорящее об отсутствии возможности делания скриншота согласно политикам безопасности. |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 | Среди exported=true провайдеров имеются следующие:  <provider android:authorities="com.spotify.mobile.android.mediaapi" android:exported="true" android:name="com.spotify.mobile.android.service.media.provider.MediaProvider"/>  <provider android:authorities="com.spotify.music.provider" android:exported="true" android:grantUriPermissions="true" android:name="com.bmwgroup.connected.car.contentprovider.AssetsProvider"/>  Первый ContentProvider предоставляет различные изображения, будь то обложка альбома или какая-то фоновая картинка.  Второй используется для обмена мультимедийной информацией с проигрывателем автомобиля BMW. |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 | C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_23-07-05.png  EditText во fragment\_login.xml – поле для ввода пароля. При вводе символы заменяются точками. |
| 1.7 | Резервное копирование STORAGE-8 | C:\Users\kiril\YandexDisk\Скриншоты\2020-03-10_23-12-33.png  Приложение не использует возможности Android для сохранения бекапа. |
| 1.8 | Фоновый режим STORAGE-9 | Выше приведены два скриншота приложения в фоновом режиме на разных экранах при тестировании приложения методом “черного ящика”. На левом скриншоте изображен экран с личным песнями пользователя, на правом экран логина, на котором вводятся логин и пароль пользователя, следовательно разработчики считают нужным скрывать данную информацию и только её как конфиденциальную.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-17_20-03-04.png  Вероятно, в данном участке кода класса LoginActivity устанавливается флаг, который предотвращает показ конфиденциальной информации в фоновом режиме. |
| 1.9 | Хранение конфиденциальных данных в памяти STORAGE-10 | Конфиденциальные данные, в виде логина и пароля, используются в LoginActivity, SpotifyService и HTTP клиенте. Активити отвечает за обработку непосредственно на экране. За процесс аутентификации отвечает сервис, посылая запрос на сервер, используя HTTP клиент. Таким образом данные используются в минимальном количестве компонент, только в необходимых. Однако обращение с конфиденциальными данными происходит не самым лучшим образом. Данные представляются типом String, данные никак не затираются и не удаляются из пула, ссылки не перезаписываются. Вместо этого стоит использовать массивы, например, ByteArray или CharArray, и стирать данные из памяти сразу же после их использования.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-17_22-32-31.png |
| 1.10 | Требование настройки доступа к устройству  STORAGE-11 | Следов использования Settings.Secure или Device Administration API найдено не было. |
| 1.11 | Проверка сертификатов  NETWORK-3 | Поиск в коде по TrustManager или HostnameVerifier не дал результатов.  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-29_14-27-48.png  Приложение не подлежит отладке, следовательно по умолчанию ошибки TLS не будут игнорироваться. |
| 1.12 | Проверка SSL PINNING  NETWORK-4 | C:\Users\kiril\YandexDisk\Скриншоты\2020-03-29_14-36-26.png  C:\Users\kiril\YandexDisk\Скриншоты\2020-03-29_14-38-57.png  Конфигурационного файла для сетевых настроек обнаружено не было. |
| 1.13 | Наличие доверительного канала связи  NETWORK-5 | Для регистрации в приложении возможна исключительно опция с электронной почтой. Для восстановления аккаунта соответсвтенно возможно опция с отправкой на электронный адрес, указанный при регистрации. |
| 1.14 | SECURITY PROVIDER  NETWORK-6 | Доступа к файлам сборки не имеется. |
| 1.15 | Реализация аутентификации на стороне сервера AUTH-1 | В качестве дополнительных факторов авторизации приложение использует геолокацию, IP адрес и используемое устройство. Приложение позволяет авторизовываться из страны, не совпадающей с указанной страной проживания, максисмум в течение 2 недель. Также различается авторизация в зависимости от устройства, что повзоляет использовать дополнительные функции внутри приложения. |
| 1.16 | Управление сеансом с отслеживанием состояния AUTH-2 | На стороне сервера токены генерируются случайным образом.  Кажется, что угадать их невозможно. Доступ к ендпоинтам на сервере производится по защищенному подключению. В исходном коде не было найдено следов сохранения в какой-либо вид постоянного хранилища информации о токене.  C:\Users\kiril\YandexDisk\Скриншоты\2020-04-21_22-53-20.png |
| 1.17 | Управление сеансом без отслеживания состояния AUTH-3 | Удалось убедиться, что токены хранять в KeyStore. |
| 1.18 | Тестирование выхода пользователей из системы AUTH-4 | Не нашел возможности проверить данный пункт. |
| 1.19 | Реализация парольной политики AUTH-5 | Ограничения на пароль отвечают требованиям о длине, обрезке, использовании всех символов и чередовании учетных данных. |
| 1.20 | Защита от перебора данных авторизации AUTH-6 | Элементы управления реализованы на сервере, а при большом количестве неудавшихся попыток начинает появляться капча, добиться блокировки не удалось. |
| 1.21 | Срок действия токена AUTH-8 | По результатам тестирования оказалось, что времени ожидания не существует, а следовательно данный тест не пройден. |
| 1.22 | Двухфакторная аутентификация AUTH-9 AUTH-10 | В приложении не предусмотрена двухфакторная аутентификация. |
| 1.23 | Информирование пользователя о действиях с его учётной записью AUTH-11 | В результате обзора и тестирования различных сценариев с заходом в приложение с новых устройств, сменой паролей, никаких дополнительных push-уведомлений или электронных писем не приходит. |