Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | Microsoft to do list |
| Версия | | 2.11.148 |
| Дата проверки | | 02.03.2020 |
| Проверил | | Рай Александр |
| Конфиденциальная информация | | Списки задач, напоминалки, пароль и логин учетной записи Microsoft |
| **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 | + В файле AndroidManifest.xml присутствуют разрешения на чтение и запись во внешнее хранилище |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | + В файле AndroidManifest.xml отсутствуют права доступа к файлам MODE\_WORLD\_READABLE и MODE\_WORLD\_WRITABLE |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | Среди всех классов и функций присутствует только класс SharedPreferences |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | Не удалось получить доступ к файлам, т.к. был доступен лишь apk файл. |
| 1.1.5 | файлы ресурсов | Не было обнаружено подозрительных строк. |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | Разработчики используют класс android.util.Log, но не передают туда конфиденциальных данных. Логируются только ошибки |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 | В приложении используется библиотека Retrofit.  Передача конфиденциальных данных сторонним приложениям не выявлена. |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 | Подсказки появляются при вводе логина. При вводе пароля подсказок нет. |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 | Тег exported для всех провайдеров установлен как false.  Теги android:permission для провайдеров не установлены.  Атрибут protectionLevel не установлен. |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 | При вводе пароля он маскируется точками. |
| 1.7 | Резервное копирование STORAGE-8 | Флаг allowBackup установлен в false  Приложение не использует возможности Android для сохранения бекапа. |
| 1.8 | Фоновый режим STORAGE-9 | При входе в фоновый режим конфиденциальные данные не скрываются. |
| 1.9 | Хранение конфиденциальных данных в памяти STORAGE-10 | - |
| 1.10 | Требование настройки доступа к устройству  STOTAGE-11 | Settings.Secure, во всей видимости, не используется. |
| 1.11 | Проверка сертификатов X.509  (NETWOR- 3) | Верифицирует  Следов HostnameVerifier в приложении не найдено. |
| 1.12 | ПРОВЕРКА SSL PINNING  (NETWORK‑4) | Файл конфигурации отсутствует. |
| 1.13 | TRUST ANCHORS  (NETWORK‑4) | Файл *network\_security\_config.xml* отсутствует. |
| 1.14 | НАЛИЧИЕ ДОПОЛНИТЕЛЬНОГО КАНАЛА СВЯЗИ  (NETWORK‑5) | Отсутствует |
| 1.15 | SECURITY PROVIDER  (NETWORK‑6) | Отсутствует доступ к файлам сборки. |
| 1.16 | РЕАЛИЗАЦИЯ АУТЕНТИФИКАЦИИ НА СТОРОНЕ СЕРВЕРА  AUTH-1 | Дополнительные факторы аутентификации отсутствуют |
| 1.17 | Управление сеансом с отслеживанием состояния AUTH-2 | Не нашел возможности проверить |
| 1.18 | Управление сеансом без отслеживания состояния AUTH-3 | Не нашел возможности проверить |
| 1.19 | Тестирование выхода пользователей из системы AUTH-4 | Код сервера не доступен. |
| 1.20 | Реализация парольной политики AUTH-5 | +минимальная длина пароля не менее 8 символов;  − максимальная длина пароля не более 128 символов;  + не происходит «обрезка» паролей. Убедитесь, что каждый символ, который вводит пользователь, действительно включен в пароль;  + разрешено использование всех символов, включая юникод и пробелы. Не должно быть правил составления пароля, ограничивающих тип разрешенных символов;  − обеспечивается чередование учетных данных. |
| 1.21 | Защита от перебора данных авторизации AUTH-6 | Счетчик отсутствует |
| 1.22 | Срок действия токена AUTH-8 | Не реализован |
| 1.23 | Двухфакторная аутентификация AUTH-9 AUTH-10 | В приложении не предусмотрена двухфакторная аутентификация |
| 1.24 | Информирование пользователя о действиях с его учётной записью AUTH-11 | Отсутствует |
| 1.25 | ЛОКАЛЬНАЯ АУТЕНТИФИКАЦИЯ В ANDROID  ПОДТВЕРЖДЕНИЕ УЧЕТНЫХ ДАННЫХ | Отсутствует |
| 1.26 | ЛОКАЛЬНАЯ АУТЕНТИФИКАЦИЯ В ANDROID  БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ  FINGERPRINTMANAGER | Отсутствует |
| 1.27 | ТРЕБОВАНИЯ К КРИПТОГРАФИИ  ПРОВЕРКА ИСПОЛЬЗОВАНИЯ СТАНДАРТНЫХ КРИПТОГРАФИЧЕСКИХ  АЛГОРИТМОВ (CRYPTO-2, CRYPTO-3, CRYPTO-4) | Используются Mac, MessageDigest |
| 1.28 | ТРЕБОВАНИЯ К КРИПТОГРАФИИ  ТЕСТИРОВАНИЕ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ (CRYPTO-6) | Класс Random не используется |
| 1.29 | Проверка на уязвимости к инъекциям фрагментов  PLATFORM-2 | Отсутствуют |
| 1.30 | Проверка пользовательских URL SCHEMES PLATFORM-3 | Пользовательские схемы URL не определены. |
| 1.31 | Проверка безопасной работы приложения при использовании IPC PLATFORM-4 | exported сервисы используются, но утечки данных нет. |
| 1.32 | Проверка выполения Javascript в WebViews PLATFORM-5 | WebView отсутствует |
| 1.33 | Требования к взаимодействию с операционной системой  PLATFORM-6 | WebView отсутствует |
| 1.34 | Требования к взаимодействию с операционной системой  PLATFORM-7 | WebView отсутствует |
| 1.35 | Проверка сохранения объектов PLATFORM-8 | Сохранение объекта не используется для хранения  конфиденциальной информации на устройстве |
| 1.36 | ПРИЛОЖЕНИЕ ПОДПИСАНО ВАЛИДНЫМ  СЕРТИФИКАТОМ (CODE-1) | Релизная сборка подписана с использованием всех трех схем |
| 1.37 | ВОЗМОЖНОСТЬ ОТЛАДКИ ПРИЛОЖЕНИЯ (CODE-2) | Возможность отладки отсутствует. |
| 1.38 | ПРОВЕРКА НАЛИЧИЯ УЯЗВИМОСТЕЙ В  СТОРОННИХ БИБЛИОТЕКАХ (CODE-5) |  |
| 1.39 | ПРОВЕРКА ОБРАБОТКИ ИСКЛЮЧЕНИЙ  (CODE-6, CODE-7) | Приложение не предоставляет конфиденциальную информацию при  обработке исключений в своем пользовательском интерфейсе или в логах. |
| 1.40 | ПРОВЕРКА АКТИВАЦИИ СТАНДАРТНЫХ ФУНКЦИЙ  БЕЗОПАСНОСТИ (CODE-9) |  |