

Исследование защищенности мобильных приложений для выбора недвижимости

Дом с сюрпризом: уязвимости мобильных приложений для выбора недвижимости

«Ростелеком-Солар» представил результаты исследования защищенности мобильных приложений для аренды и покупки недвижимости. Для анализа были выбраны наиболее популярные в категории «Недвижимость» программы, представленные на мобильных платформах **Android** и **iOS**: «Циан», «ДомКлик», «Яндекс.Недвижимость», **N1.RU**, **Domofond**, **Airbnb**, **Mitula**, «Этажи», **Indomio**, **idealista** ^[1].

Среди уязвимостей, наиболее часто встречающихся в этих приложениях, были обнаружены те, что потенциально могут привести к нелегитимному доступу к системе и компрометации конфиденциальных данных пользователей. **Объектами кражи могут стать ФИО, ежемесячный доход, паспортные данные и другая ценная информация.**

Согласно полученным в ходе анализа данным, «Domofond Недвижимость. Квартиры: новостройки, дом» – наиболее защищенное приложение ^[2] для выбора недвижимости на платформе Android. На втором и третьем месте расположились «Indomio: продажа и аренда дом в Италии, Испании» и **idealista**. Их показатели выше среднего по сегменту уровня защищенности, который на момент подготовки исследования составил 2.2 балла из 5.0.

Самый высокий показатель общего уровня защищенности из всех проанализированных приложений на платформе iOS продемонстрировал **Airbnb**. Общий уровень защищенности этого сервиса для платформы iOS оценивается в 4.0 балла из 5.0, что значительно выше, чем у остального анализируемого ПО.

Уязвимости Android-приложений

Сканирование показало, что чаще всего в приложениях для выбора недвижимости на платформе Android встречаются такие известные уязвимости, как «Обход проверок безопасности SecurityManager» (занимает долю 38% от общего количества), «Использование JNI» (16%), «Некорректная работа с потоками» (6%).

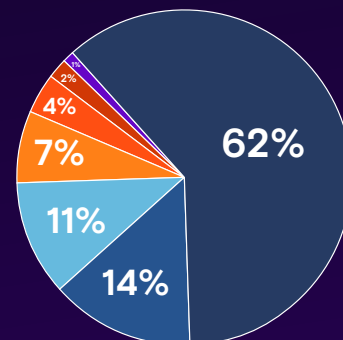


Основная угроза описанных проблем безопасности в том, что они могут привести к утечкам конфиденциальных данных пользователей сервисов.

Уязвимости iOS-приложений

Анализ iOS-приложений категории «Недвижимость» показал, что в них наиболее часто встречаются такие уязвимости, как **«Небезопасная рефлексия»** (занимает долю 42% от общего количества), **«Слабый алгоритм шифрования»** (30%), **«Использование NSLog»** (9%).

- ◆ 62% – Небезопасная рефлексия
- ◆ 14% – Использование NSLog
- ◆ 11% – Использование метода openURL
- ◆ 7% – Использование незащищённого протокола HTTP
- ◆ 4% – Небезопасное хранение данных
- ◆ 2% – Некорректное использование API UNIX
- ◆ 1% – Другое



Наиболее распространенные виды уязвимостей в мобильных приложениях для выбора недвижимости на iOS

Согласно результатам анализа, мобильные приложения для выбора недвижимости, разработанные для платформы iOS, значительно хуже защищены, чем их Android-аналоги. Однако, по мнению экспертов, это частично компенсируется более высокой защищенностью мобильной операционной системы Apple Inc. Количество вхождений критических уязвимостей в приложениях на iOS в 30 раз выше, чем аналогичный показатель у Android.



Наиболее часто перечисленные уязвимости эксплуатируются в целях кражи персональных данных.

«Общий уровень защищенности приложений в категории “Недвижимость” и тот факт, что iOS и Android-приложения содержат критические уязвимости, вызывает серьезные опасения,— отмечает **Даниил Чернов, директор Центра Solar sppScreener компании «Ростелеком-Солар»**. — Исследуемые программы обрабатывают такие данные, как ФИО, дата рождения, семейное положение, информация о детях, ежемесячный доход, а также паспортные данные (серия, номер, дата выдачи, код подразделения, наименование органа, выдавшего паспорт, регистрация). Уязвимости приложений могут привести к утечке этих данных, что повлечет за собой крайне негативные последствия для пользователей. Подобные риски подчеркивают высокую необходимость внедрения безопасного процесса разработки программного обеспечения».



Анализ безопасности кода осуществлялся автоматически с помощью Solar appScreener – российского программного продукта для проверки защищенности приложений. Решение использует методы статического, в том числе бинарного, анализа. При подготовке исследования модуль декомпиляции и деобфускации был отключен. Статический анализ производился в отношении бинарного кода мобильных приложений в автоматическом режиме с автоматической верификацией модулем Fuzzy Logic Engine.

[1] Для сравнения уровня защищенности были выбраны популярные мобильные приложения для аренды и покупки недвижимости – «Циан. Недвижимость. Квартиры» для iOS v. 1.205; «Циан. Недвижимость: квартиры, новостройки, ипотека» для Android v. 2.205.0; «ДомКлик. Снять, купить квартиру iOS v. y» для Android v. 8.28.48.27.0; «ДомКлик. Недвижимость: купить, снять квартиру, дом» для ; «Яндекс. Недвижимость Android v. 5.2.0» квартиры» для –Яндекс.Недвижимость iOS v. 5.2; «ь» для ; «N1.RU Недвижимость Android Недвижимость: квартиры, новостройки, жильё» для –.RU iOS v. 5.4.6; «N1» для (версия зависит от устройства); «Domofond Недвижимость:квартир iOS v. 11; «Domofond ы» для Android v. 17 Недвижимость. Квартиры: новостройки, дом» для ; Airbnb для iOS v. 21.38; Airbnb для Android v. 21.37; «Mitula Недвижимость Android v. 5.4» для Недвижимости iOS v. 5.2.0; «Mitula ь» для , «Этажи, недвижимость и ипотека Android v. Этажи: квартиры, новостройки, ипотека» для iOS v. 1.39.0; «а» для 2.39.0.20210901; «Indomio: Поиск дома» для iOS v. 8.12.2; «Indomio: продажа и аренда дом в Италии, Испании» для Android v. 5.6.5; idealista для iOS v. 10.5.6; idealista для Android v. 9.5.3.

[2] Оценка защищенности приложения высчитывается автоматически и учитывает такие показатели, как количество различных типов известных уязвимостей критического и среднего уровня и частота их повторяемости (количество вхождений) в коде. Вклад количества критических уязвимостей более высок, при этом он не учитывает объем кода. Количество уязвимостей среднего уровня учитывается с поправкой на объем кода. Число вхождений уязвимостей в конкретных приложениях в рамках данного исследования не раскрывается.



rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70