Ростелеком
Солар

Исследование защищенности мобильных приложений для выбора алкоголя. Декабрь 2019.

Официальная информация (disclaimer)

Данный отчет был подготовлен (ООО «СОЛАР СЕКЬЮРИТИ») (далее - компания «Ростелеком-Солар») с целью исследования и испытания функциональности популярных мобильных приложений для выбора алкоголя. Отчет может быть использован исключительно в информационных целях.

Информация, полученная в результате проведенного исследования и изложенная в отчете, была получена при использовании технологии автоматического бинарного анализа, без выполнения реверс-инжиниринга (декомпиляции исходного кода).

Иная содержащаяся в настоящем отчете информация была получена из источников, которые, по мнению «Ростелеком-Солар», являются надежными, однако «Ростелеком-Солар» не гарантирует точности и полноты информации для любых целей.

Все упомянутые в отчете товарные знаки являются собственностью их владельцев.

Информация, представленная в этом отчете, не должна быть истолкована прямо или косвенно как информация, содержащая рекомендации «Ростелеком-Солар» по инвестициям или использованию программных решений. Все мнения и оценки, содержащиеся в настоящем материале, отражают мнение авторов на день публикации и подлежат изменению без предупреждения.

«Ростелеком-Солар» не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в данном отчете, включая опубликованные мнения или заключения, а также за последствия, вызванные неполнотой или неточностью представленной информации.

Дополнительная информация предоставляется по запросу.

Методология

Для сравнения уровня защищенности были выбраны популярные мобильные приложения для выбора алкогольных напитков – Vivino[1], Simple Wine[2], Untappd[3], Виски[4], Whisky Suggest[5], «Мой Коктейль Бар»[6], «Коктейли-рецепты для вечеринки»[7], Красное&Белое[8], КуулКЛЕВЕР («Отдохни»)[9], Бристоль[10], «Ароматный Мир»[11] и «ВинЛаб»[12].

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

Проанализировав приложения, Solar appScreener сформировал отчеты, в которых была приведена общая оценка защищенности приложения по пятибалльной системе, список обнаруженных закладок, **известных** уязвимостей и ошибок, ранжированных по уровню критичности. Эти отчеты легли в основу данного исследования.

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.

Основываясь на выборке из последних 500 сканирований, Solar appScreener рассчитывает средний по отрасли уровень защищенности приложений. На момент подготовки отчета он составлял 2,2 балла.

---

[1] Vivino: Buy the Right Wine for iOS v. 8.18.13; Vivino – сканер вина for Android v. 8.18.22
[2] SimpleWine – вино и напитки for iOS v. 1.1.7; SimpleWine - вино и напитки от сомелье for Android v. 1.1.72
[3] Untappd - Discover Beer for iOS v. 3.4.8; Untappd - Discover Beer for Android v. 3.4.8
[4] Виски for Android v. 1.0.3
[5] Whisky Suggest for iOS v. 2.16
[6] Мой Коктейль Бар for Android (версия зависит от устройства)
[7] Коктейли-рецепты для вечеринки for iOS v. 4.4
[8] Красное&Белое for iOS v. 2.17.3; Красное&Белое — магазин, акции for Android v. 2.17
[9] КуулКЛЕВЕР (Отдохни) for iOS v. 1.2; КуулКЛЕВЕР (Отдохни) (версия зависит от устройства)
[10] Приложение Bristol for iOS v. 1.3; Бристоль for Android v. 1.0.5
[11] Ароматный Мир for iOS v 2.12, Ароматный Мир for Android v. 3.2.14
[12] WineLab for iOS v. 1.0.45, ВинЛаб for Android v. 1.0.45

Введение

Компания «Ростелеком-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет сравнение защищенности наиболее популярных мобильных приложений для выбора алкоголя.

В настоящее время в Российской Федерации действует ограничение на продажу алкогольных напитков через Интернет, введенное постановлением правительства в 2007 году. Это ограничение не раз становилось предметом бурных дискуссий. В результате Министерство финансов РФ в декабре 2019 планирует внести в Правительство РФ законопроект о легализации онлайн-продажи алкоголя. Согласно тексту документа, онлайн-торговля алкоголем начнется с 1 января 2020 года[13] и на первом этапе (до января 2021 г.) будет распространяться лишь на вина и лишь для их производителей или оптовых компаний.

Основной целью законопроекта обозначена борьба с теневым оборотом спиртного в рунете. По данным компании Group-IB, нелегальные продажи алкоголя в интернете в России за 2018 год выросли на 23%, до 2,1 млрд руб. Эксперты обнаружили 4 тыс. сайтов, торговавших алкоголем через интернет в 2018 году, в 2017 году они фиксировали 3 тыс. подобных сайтов.

В связи с ростом актуальности тематики выбора и покупки алкоголя онлайн и в преддверие новогодних праздников эксперты компании «Ростелеком-Солар» провели исследование уровня защищенности популярных мобильных приложений для выбора алкоголя с помощью инструмента Solar appScreener.

Сервисы для анализа были отобраны согласно критерию популярности: количеству скачиваний и занимаемому месту в разделе «Еда и напитки» в Google Play и App Store. В исследовании приняли участие приложения для выбора напитков следующих категорий: вино, пиво, виски и коктейли.

Это первое исследование, которое рассматривает угрозы информационной безопасности мобильных приложений для выбора алкогольных напитков – от недостаточно надежных методов защиты паролей до уязвимости приложений к различным типам известных атак и эксплойтов.

[13] РБК. Минфин предложил разрешить онлайн-продажу алкоголя с 2020 года

Найденные ошибки и потенциальные уязвимости

Сканирование показало, что чаще всего в приложениях для выбора алкоголя встречаются такие известные уязвимости, как *слабые алгоритмы хеширования, использование пустых паролей в исходном коде, обход проверок безопасности SecurityManager, использование NSLog*. При этом по результатам анализа выяснилось, что лишь одно приложение и всего списка – «SimpleWine - вино и напитки от сомелье» – не содержит критические уязвимости.

Анализ приложений под Android выявил, что 90% из них допускает обход проверок безопасности SecurityManager. 80% исследованных Android-приложений допускают внутреннюю утечку ценной информации. Наконец, в 30% Android-версий использованы пустые пароли в исходном коде.

Для iOS-версий мобильных приложений, предназначенных для выбора алкоголя, характерны такие уязвимости, как использование небезопасной хеш-функции, «отладочного» метода NSLog, а также метода, реализующего рефлексию (принимает данные из недоверенного источника). Этим уязвимостям подвержены все исследованные мобильные сервисы для iOS.

Ниже подробно рассмотрены уязвимости, наиболее часто встречающиеся в исследованных приложениях.

СЛАБЫЙ АЛГОРИТМ ХЕШИРОВАНИЯ

Использованная в приложении хеш-функция не является безопасной и может привести к утрате конфиденциальности данных.

Хеш-функции представляют собой инструмент криптографии для выполнения самых разных задач – аутентификации, проверки целостности данных, защиты файлов и многого другого. Алгоритмы хеширования отличаются криптостойкостью, сложностью и другими параметрами.

Некоторые хеш-функции имеют известные уязвимости, и нахождение коллизий для них не является трудоемкой задачей. Соответственно, если эти функции применяются для хранения ценной информации (например, паролей), её конфиденциальность может быть нарушена. Хеш-функция, используемая для хранения паролей, помимо устойчивости к коллизиям, должна быть не слишком быстрой, чтобы осложнять атаку путём полного перебора.

Приведем пример атаки с использованием данной уязвимости. Пусть пароли пользователей хранятся на сервере в зашифрованном виде с использованием небезопасной хеш-функции. Сначала злоумышленник получает доступ к базе зашифрованных паролей. Затем, используя уязвимость алгоритма хеширования, он вычисляет строку, для которой алгоритм хеширования даёт то же значение, что и для пароля пользователя. Затем злоумышленник проходит аутентификацию, используя вычисленную строку.

Данная уязвимость содержится **в каждом исследованном iOS-приложении для выбора алкоголя**.

Рекомендации разработчикам: необходимо использовать надёжные функции хеширования (SHA-2). Для хеширования паролей - использовать специализированные хеш-функции (PBKDF2, bcrypt, scrypt) и полученную из криптографически стойкого генератора псевдослучайных чисел соль.

ИСПОЛЬЗОВАНИЕ NSLOG

Использовать этот метод можно в процессе отладки программного обеспечения, но никак не на стадии коммерческой эксплуатации приложения. Все сообщения, генерируемые с помощью NSLog, можно просмотреть посредством XCode (среды разработки ПО под iOS). В результате может быть раскрыта информация, которая позволит злоумышленнику реализовать атаку на

приложение. Уже не говоря о том, что активное использование NSLog серьезно замедляет работу приложения.

Данным видом уязвимости охвачены **также все iOS-версии исследованных приложений**.

Рекомендации разработчикам: отключайте NSLog в коммерческой версии приложений с помощью макросов препроцессора.

НЕБЕЗОПАСНАЯ РЕФЛЕКСИЯ

С помощью небезопасной рефлексии злоумышленник может взять приложение под свой контроль, обойти механизмы аутентификации и ограничения доступа и выполнить произвольный вредоносный код, поскольку этот метод принимает в качестве аргумента данные из недоверенного источника.

Если рефлексия используется для вызова произвольного кода, это может привести к завершению работы приложения или зависанию. Вызвав неправильный код, злоумышленник инициирует ошибку времени выполнения, которая приводит к утечке конфиденциальной информации в сообщении об ошибке.

Уязвимости типа «подделка кода» (Code Tampering) занимают **восьмое место в рейтинге уязвимостей приложений «OWASP Mobile Top 10».**

Метод, реализующий рефлексию, встречается в **100% проанализированных iOS-приложений.**

Рекомендации разработчикам: составьте белый список допустимых команд и предоставьте пользователю возможность выбирать только из этого списка. Не используйте напрямую данные, введённые пользователем, в качестве аргумента методов, реализующих рефлексию.

ОБХОД ПРОВЕРОК БЕЗОПАСНОСТИ SECURITYMANAGER

Приложение допускает небезопасный вызов метода из недоверенного кода. В результате злоумышленник получает доступ к пакету с ограниченным доступом и может выполнять произвольный код.

Небезопасный вызов метода из недоверенного кода позволяет обойти проверки безопасности SecurityManager, контролирующие наличие достаточных привилегий по всей цепочке вызовов. В результате один из элементов цепочки может получить доступ к ресурсу, не обладая достаточными на то правами.

Данная уязвимость содержится **в 9-ти из 10-ти исследованных Android-приложениях**.

Рекомендации разработчикам: убедитесь, что важные методы программного интерфейса приложения не доступны для вызова из недоверенного кода. Не используйте объекты, возвращаемые этими методами, в недоверенном коде.

ВНУТРЕННЯЯ УТЕЧКА ЦЕННОЙ ИНФОРМАЦИИ

В случае утечки подробной информации о конфигурации системы внутренний злоумышленник может воспользоваться этими данными для разработки плана атаки.

В зависимости от настроек приложения техническая информация и сообщения об ошибках в приложении могут фиксироваться в журнале, выводиться в консоль управления или передаваться пользователю. В некоторых случаях внутренний злоумышленник, например, сотрудник компании-разработчика или заказчика системы по сообщению об ошибке может узнать об имеющейся в приложении уязвимости. Например, ошибка базы данных может свидетельствовать об уязвимости к атакам типа SQL injection. Информация о версии операционной системы, сервера приложений или конфигурации системы может послужить для планирования атаки. Поэтому следует

исключить из внутренних сообщений об ошибках слишком подробную техническую информацию о системе и её конфигурации.

Этот вид уязвимости встречается **в 8-ми из 10-ти проанализированных приложений для ОС Android**.

Рекомендации разработчикам: исключите из сообщений об ошибках излишне подробную информацию о системе и её конфигурации.

ПУСТОЙ ПАРОЛЬ

Пустой пароль может привести к компрометации приложения. Устранить угрозы безопасности, связанные с заданными в исходном коде пустыми паролями, очень сложно. Информация о том, что определённая учётная запись принимает пустой пароль, как минимум, доступна каждому разработчику приложения. Более того, после установки приложения удалить из его кода пустой пароль можно только посредством обновления. Константные строки легко извлекаются из скомпилированного приложения декомпиляторами. Поэтому злоумышленнику не обязательно иметь доступ к исходному коду, чтобы узнать параметры специальной учётной записи. Если эти параметры станут известны злоумышленнику, администраторам системы придётся либо пренебречь безопасностью, либо ограничить доступ к приложению.

Эта критичная уязвимость занимает **7-е место в рейтинге «2019 CWE Top 25 Most Dangerous Software Errors».**

Данная уязвимость содержится в **3-х из 10-ти исследованных приложений на базе Android.**

Рекомендации разработчикам: крайне не рекомендуется использовать пустые пароли в коде: следует хранить не пароли, а значения криптографически стойкой хеш-функции от паролей. Необходимо хранить аутентификационную информацию в зашифрованном виде в отдельном конфигурационном файле или в базе данных.

Сравнительный анализ безопасности мобильных приложений для выбора алкоголя

Оценка защищенности приложения высчитывается автоматически и учитывает такие показатели, как количество различных типов известных уязвимостей критического и среднего уровня и количество их повторений (вхождений) в коде.

Уровень защищенности Android-версий:

Приложение	Критические уязвимости (кол-во уникальных)	Критические уязвимости (кол-во вхождений)	Уязвимости среднего уровня (кол-во уникальных)	Уязвимости среднего уровня (кол-во вхождений)	Общий уровень защищенности
SimpleWine - вино и напитки от сомелье	0	0	38	606	3.8/5.0
Ароматный Мир	1	1	30	308	3.2/5.0
Vivino - сканер вина	1	1	31	562	3.1/5.0
Untappd - Discover Beer	1	2	10	273	2.9/5.0
Виски	2	2	23	257	2.9/5.0
Красное&Белое — магазин, акции	2	2	41	408	2.8/5.0
Мой Коктейль Бар	1	4	37	530	2.3/5.0
КуулКЛЕВЕР (Отдохни)	5	7	29	289	2.0/5.0
Бристоль	2	2	32	10208	1.9/5.0
ВинЛаб	3	7	36	598	1.9/5.0

Из сравнительной таблицы видно, что безусловным лидером по уровню защищенности среди Android-приложений для выбора алкоголя является приложение «SimpleWine - вино и напитки от сомелье». Данное приложение не содержит ни одной критической уязвимости, его показатель общего уровня защищенности равен 3.8 балла из 5.0. На 0,6 балла отстает от лидера приложение «Ароматный Мир» (3.2 балла) и на 0.7 балла – «Vivino - сканер вина» (3.1 балла): они содержат по одной критической уязвимости в программном коде.

Приложения для выбора алкоголя Untappd - Discover Beer, «Виски» и «Красное&Белое — магазин, акции» находятся примерно на одном уровне защищенности и демонстрируют результат выше среднего по отрасли. Еще одному приложению, «Мой Коктейль Бар» (2.3 балла), удалось пересечь отметку в 2.2 балла – средний по отрасли показатель уровня защищенности.

Android-версии приложений «КуулКЛЕВЕР (Отдохни)» и «ВинЛаб» содержат в исходном коде по 7 вхождений критических уязвимостей, что превышает предельно допустимый показатель в 5 единиц, чтобы не опуститься ниже среднего по рыку общего уровня защищенности. Это не позволяет считать данные приложения безопасными для использования.

В данном исследовании впервые наблюдается ситуация, когда приложение (Бристоль), содержащее в исходном коде всего 2 вхождения критических уязвимостей, получает низкую оценку общего уровня защищенности по причине огромного количества вхождений уязвимостей среднего уровня (10208!)

Уровень защищенности iOS-версий:

Приложение	Критические уязвимости (кол-во уникальных)	Критические уязвимости (кол-во вхождений)	Уязвимости среднего уровня (кол-во уникальных)	Уязвимости среднего уровня (кол-во вхождений)	Общий уровень защищенности
КуулКЛЕВЕР (Отдохни)	2	10	7	425	1.6/5.0
Приложение Bristol	1	12	5	176	1.5/5.0
SimpleWine – вино и напитки	1	12	6	205	1.5/5.0
Whisky Suggest	1	13	6	446	1.4/5.0
Vivino: Buy the Right Wine	1	20	7	603	1.1/5.0
Ароматный мир	2	26	6	777	0.8/5.0
Красное&Белое	1	32	7	551	0.7/5.0
Коктейли-рецепты для вечеринки	1	40	5	42	0.6/5.0
Untappd - Discover Beer	2	45	8	1184	0.4/5.0
Winelab	1	59	9	957	0.3/5.0

Результаты, представленные в таблице, свидетельствуют о крайне низком уровне защищенности мобильные приложений для выбора алкоголя, разработанных под операционную систему iOS, по сравнению с их Android-аналогами. Столь низкие показатели объясняются на порядок бОльшим количеством вхождений уязвимостей критического уровня в iOS-версиях по сравнению с соответствующими Android-приложениями. Что, однако, в некоторой степени компенсируется более высокой защищенностью самой операционной системы.

Самые лучшие показатели продемонстрировало iOS-приложение «КуулКЛЕВЕР (Отдохни)», однако и оно по результатам тестирования набрало лишь 1.6 балла, что значительно ниже среднего по отрасли показателя в 2.2 балла. Приложение Winelab включает самое большое количество вхождений уязвимостей критического уровня. Поэтому по результатам автоматизированной проверки с помощью Solar appScreener оно получило самый низкий балл – 0.3 балла из 5.0.

Выводы

Исследование защищенности мобильных приложений для выбора алкоголя показало, что Android-версии проанализированных мобильных сервисов отличаются более высокой защищенностью, чем их iOS-аналоги.

По итогам сканирования в приложениях обнаружен ряд уязвимостей, потенциально ведущих к компрометации обрабатываемых данных. В частности, паролей от учетных записей пользователей в соцсетях, поскольку многие из исследованных приложений поддерживают аутентификацию через соцсети. В результате злоумышленник может получить доступ к переписке пользователя, а также конфиденциальной информации, содержащихся в социальном аккаунте.

Кроме того, некоторые из исследованных приложений могут допускать утечку технической информации о конфигурации приложений. Это потенциально позволяет злоумышленнику совершать атаку на приложение, например, внедрить вредоносный код, а также, получив контроль над приложением, совершать атаки на другие системы.

Сканирование приложений под Android показало, что 9 из 10-ти приложений допускают небезопасный вызов метода из недоверенного кода, что может быть использовано злоумышленником для выполнения произвольного кода. 8 из 10-ти исследованных Android-приложений допускают внутреннюю утечку информации о конфигурации системы, что облегчает злоумышленнику организацию атаки на приложение. А в трех случаях использованы пустые пароли в исходном коде, что может привести к компрометации приложения в целом.

Все исследованные iOS-приложения для выбора алкоголя содержат хеш-функции, обладающие известными уязвимостями, эксплуатация которых может привести к нарушению конфиденциальности данных пользователей. Также в 100% проанализированных приложений на базе iOS применен «отладочный» метод NSLog, благодаря чему может быть раскрыта информация, которая позволит злоумышленнику реализовать атаку на приложение. А по причине применения небезопасной рефлексии все исследованные iOS-приложения для выбора алкоголя потенциально уязвимы к выполнению произвольного вредоносного кода, поскольку этот метод принимает в качестве аргумента данные из недоверенного источника.

По результатам автоматизированного сканирования с помощью Solar appScreener, самым защищенным Android-приложением для выбора алкоголя признано приложение «SimpleWine - вино и напитки от сомелье». А наиболее уязвимым – приложение «ВинЛаб».

Как показало автоматизированное сканирование Solar appScreener, среди iOS-версий исследованных приложений нет ни одного, удовлетворяющего хотя бы среднему по отрасли уровню защищенности. Приложение WineLab продемонстрировало наиболее низкий среди всех iOS-версий результат общего уровня защищенности – 0.3 балла из 5.0