Апрель 2020

Исследование защищенности мобильных фитнес-приложений

Ростелеком Солар

appScreener

Официальная информация (disclaimer)

Данный отчет был подготовлен компанией «Ростелеком-Солар» с целью исследования и испытания функциональности популярных мобильных приложений для занятия фитнесом и спортом. 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 занятий фитнесом и спортом – Mi FIT[1] , Fitness Online[2] , Endomondo[3], Workout Trainer[4] , 7 Minute Workout: Fitness App[5] , «Фитнес-план 30 дней»[6] , Fitness Point[7] , Daily Workouts Fitness Trainer[8] , PEAR - Personal Fitness Coach[9] , «Тренировки дома - фитнес тренер» (Abishkking Limited)[10] , «7 Минут Упражнение» (Simple Design Ltd.)[11] , JEFIT[12] , Freeletics Training Coach[13] , NTC (Nike, Inc)[14] , «Тренировки для Дома» (Leap Fitness Group)[15] , «Фитнес и Бодибилдинг» (VGFIT LLC) [16].

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] Mi FIT for iOS v. 4.0.16; Mi FIT for Android v. 4.0.15

[2] Fitness Online for iOS v. 1.5.0; Fitness Online for Android v. 2.6.8

[3] Endomondo for iOS v. 18.10.1; Endomondo for Android (версия зависит от устройства)

[4] Workout Trainer for iOS v 9.6; Workout Trainer for Android (версия зависит от устройства)

[5] 7 Minute Workout: Fitness App for iOS v. 4.0.2

[6] «Фитнес-план 30 дней» (Abishkking Limited) for iOS v. 2.0.15

[7] Fitness Point for iOS v. 7.5.2

[8] Daily Workouts Fitness Trainer for iOS v. 6.12

[9] PEAR - Personal Fitness Coach for iOS v. 9.2.0

[10] «Тренировки дома - фитнес тренер» (Abishkking Limited) for iOS v. 1.1.24

[11] «7 Минут Упражнение» (Simple Design Ltd.) for Android v. 1.363.109

[12] JEFIT for Android v. 10.51

[13] Freeletics Training Coach for Android v. 6.9.0

[14] NTC (Nike, Inc.) for Android (версия зависит от устройства)

[15] «Тренировки для Дома» (Leap Fitness Group) for Android v. 1.0.31

[16] «Фитнес и Бодибилдинг» (VGFIT LLC) for Android v. 2.7.1

Введение

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

Данный отчет подготовлен и опубликован в СМИ в период пандемии короновируса Covid-19. В большинстве стран мира введены жесткие карантинные меры и закрыты все объекты массового посещения, в том числе фитнес-центры. В связи с этим наблюдается рост популярности различных онлайн-сервисов и мобильных приложений, предлагающих спортивные упражнения и тренировки в домашних условиях. Так, разработчики приложений в США отмечают **резкое увеличение количества новых пользователей, а также 50% рост подписки на фитнес-программы, не требующие спортивного снаряжения.**

В соответствии с ростом актуальности тематики эксперты компании «Ростелеком-Солар» провели исследование уровня защищенности популярных мобильных приложений для занятия фитнесом и спортом (в том числе на дому), с помощью инструмента Solar appScreener. Все исследованные приложения являются бесплатными. Однако большинство из них содержит встроенные покупки на различные дополнительные программы и сервисы, а значит, собирает данные о платежах и платежных карт пользователей. Также все приложения собирают данные учетных записей пользователей, включая логины, пароли и уникальные ID. Кроме того, приложения могут запрашивать доступ к местоположению телефона пользователя, к контактам, календарю, учетным записям в социальных сетях и собирать иные персональные данные пользователей.

Сервисы для анализа были отобраны согласно критерию популярности: занимаемому месту в категории «Здоровье и фитнес» в App Store и Google Play, количеству установок не менее 5 млн, а также позициям в рейтингах «The 10 Best Fitness Apps to Download in 2020», «7 лучших фитнес-приложений для iOS» и «7 лучших фитнес-приложений для Android».

Найденные ошибки и потенциальные уязвимости

Сканирование показало, что чаще всего в приложениях для занятия фитнесом встречаются такие известные уязвимости, как слабые алгоритмы хеширования, небезопасный режим для алгоритма шифрования, использование NSLog и обход проверок безопасности SecurityManager. При этом по результатам анализа лишь два Android-приложения – **Fitness Online (Fitness Online LLC) и «Тренировки для дома» (Leap Fitness Group)** – не содержат критических уязвимостей.

Анализ приложений под Android выявил, что более 85% из них использует алгоритм шифрования с неправильным режимом, в результате чего зашифрованное сообщение может не аутентифицироваться. То есть становится невозможно определить, что используется неправильный ключ шифрования или изменен текст шифра. Кроме того, все исследованные Android-приложения допускают небезопасный вызов метода из недоверенного кода, что вкупе с некоторыми другими методами может позволить злоумышленнику выполнять произвольный код.

Для iOS-версий мобильных фитнес-приложений характерны такие уязвимости, как использование слабых алгоритмов хеширования (слабая устойчивость к коллизиям и атакам методом перебора), установка SSL-соединения с небезопасными параметрами (может привести к компрометации передаваемых данных), а также применение «отладочного» метода NSLog (сообщения можно посмотреть при помощи XCode, что может привести к излишнему раскрытию информации). 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 небезопасна и может привести к утрате конфиденциальности данных.

Хеш-функции являются инструментом 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 представляет особой сложности. 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. После чего злоумышленник проходит аутентификацию, используя вычисленную строку.

Данная уязвимость содержится **в каждом исследованном iOS-приложении для занятия фитнесом.**

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.

Небезопасные параметры SSL

Приложение устанавливает SSL-соединение с небезопасными параметрами.

Для установки защищённого соединения приложение должно проверять, что полученный сертификат соответствует запрошенному хосту, что срок сертификата не истёк и что цепочка доверия восходит к одному из заданных в системе доверенных корневых сертификатов. Отключение любой из проверок может привести к компрометации передаваемых данных.

Небезопасное взаимодействие (Insecure Communication) занимает **третье место в рейтинге уязвимостей для мобильных платформ** «OWASP Mobile Top 10».

Данная уязвимость содержится **в 100% исследованных iOS-приложений.**

Рекомендации разработчикам: проверяйте сертификат полностью при каждом установлении соединения по протоколу SSL/TLS.

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. Кроме того, 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

Поскольку этот метод принимает в качестве аргумента данные из недоверенного источника, злоумышленник может захватить управление приложением, обойти механизмы аутентификации и ограничения доступа и выполнить произвольный вредоносный код.

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.

Небезопасный режим для алгоритма шифрования

В приложении используется алгоритм шифрования AES с неправильным режимом. В результате режим может не аутентифицировать зашифрованное сообщение – в этом случае невозможно определить, что используется неправильный ключ или изменен текст шифра.

Кроме того, возможно несовпадение размера блока для алгоритма и размера блока, для которого определен режим. Для AES размер блока равен 16 байтам. Если использовать режим, определенный для блока размером отличным от 16 байтов, то возможна неправильная интерпретация режима алгоритмом.

Этот вид уязвимости детектирован **в 7-ми из 8-ми Android-приложений** для занятия фитнесом, **содержащих критические уязвимости.**

Рекомендации разработчикам: используйте CCM и GCM режимы для алгоритма AES.

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 среднего уровня критичности содержится **во всех 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 9-ми из 10-ти проанализированных приложений для ОС Android.**

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

Сравнительный анализ безопасности мобильных фитнес-приложений

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
Fitness Online	0	0	31	282	4.1/5.0
«Тренировки для Дома» (Leap Fitness Group)	0	0	34	284	4.1/5.0
Workout Trainer	2	2	32	219	2.9/5.0
Mi FIT	2	2	32	242	2.9/5.0
Freeletics Training Coach	2	3	38	351	2.6/5.0
«Фитнес и	1	4	29	306	2.4/5.0
JEFIT	2	5	28	267	2.3/5.0
Endomondo	2	5	29	313	2.2/5.0
«7 Минут Упражнение» (Simple Design Ltd.)	1	7	32	369	2.0/5.0
NTC (Nike, Inc.)	3	12	36	417	1.5/5.0

Согласно вышеприведенной сравнительной таблице результатов сканирования, наиболее защищенными Android-приложениями для занятия спортом признаны приложения Fitness Online и «Тренировки для Дома» (Leap Fitness Group). Эти приложения не содержат ни одной критической уязвимости, их показатель общего уровня защищенности равен 4.1 балла из 5.0. Неплохие результаты (заметно выше среднего по отрасли уровня в 2.2 балла) продемонстрировали приложения Workout Trainer и Mi FIT. Их общий уровень защищенности равен 2,9 балла, поскольку они содержат в программном коде лишь по 2 критичных уязвимости.

Еще четырем Android-приложениям – Freeletics Training Coach, «Фитнес и Бодибилдинг» (VGFIT LLC), JEFIT и Endomondo – удалось пересечь отметку в 2.2 балла. Таким образом их уровень защищенности можно признать удовлетворительным.

Неожиданно слабые результаты продемонстрировала Android-версия фитнес-приложения NTC торговой марки Nike, Inc. Данное приложение содержит в исходном коде 12 вхождений критических уязвимостей, что превышает предельно допустимый показатель в 5 единиц, чтобы не опуститься ниже среднего по рынку общего уровня защищенности. Это обстоятельство не позволяет считать данное приложение безопасным для использования.

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
Daily Workouts Fitness Trainer	2	19	9	564	1.0/5.0
Fitness Point	2	26	11	1067	0.8/5.0
7 Minute Workout: Fitness App	3	27	9	548	0.8/5.0
Endomondo	3	38	10	1140	0.5/5.0
«Фитнес-план 30 дней» (Abishkking Limited)	2	50	12	785	0.4/5.0
PEAR - Personal Fitness Coach	2	65	9	3765	0.2/5.0
FitnessOnline	3	72	7	341	0.2/5.0
«Тренировки дома - фитнес тренер» (Abishkking Limited)	2	77	14	1250	0.2/5.0
Workout Trainer	2	79	11	1389	0.2/5.0
Mi FIT	4	209	12	2259	0.0/5.0

По результатам, представленным в таблице, можно сделать вывод о крайне низком уровне защищенности мобильных фитнес-приложений, разработанных под операционную систему iOS, по сравнению с Android-сервисами. Столь низкие показатели объясняются на порядок бОльшим количеством вхождений уязвимостей критического уровня в iOS-версиях по сравнению с Android-приложениями. Что, однако, в некоторой степени компенсируется более высокой защищенностью самой мобильной операционной системы торговой марки Apple Inc.

Лучшие показатели продемонстрировало iOS-приложение Daily Workouts Fitness Trainer, однако и оно по результатам тестирования набрало лишь 1.0 балла, что значительно ниже среднего по отрасли показателя в 2.2 балла. iOS-приложение MiFIT (в отличие от своего Android-аналога) включает самое большое количество вхождений (209!) уязвимостей критического уровня. Поэтому по результатам автоматизированной проверки с помощью Solar appScreener оно получило самый низкий балл – 0.0 балла из 5.0.

Выводы

Исследование защищенности мобильных приложений для занятия фитнесом и спортом показало, что Android-версии проанализированных мобильных сервисов отличаются заметно более высокой защищенностью, чем их iOS-аналоги.

По итогам сканирования в приложениях обнаружен ряд уязвимостей, потенциально ведущих к компрометации обрабатываемых данных. В частности, все приложения содержат встроенные покупки, а значит, собирают данные платежных карт пользователей. Также исследованные приложения собирают данные учетных записей пользователей в приложении, включая логины, пароли и уникальные ID. Кроме того, приложения могут запрашивать доступ к местоположению телефона пользователя, к контактам, календарю, учетным записям в социальных сетях.

В случае успешной эксплуатации ряда выявленных уязвимостей злоумышленник может получить доступ к данным банковских карт пользователей, переписке и персональным данным пользователей в их социальных аккаунтах, персональным данным других людей в контактах смартфонов пользователей фитнес-приложений и другой чувствительной информации.

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.

По результатам автоматизированного сканирования с помощью Solar appScreener, самыми защищенными Android-приложениями для занятий фитнесом признаны приложения Fitness Online и «Тренировки для Дома» (Leap Fitness Group).
А наиболее уязвимым – приложение NTC (Nike, Inc.)

Как показало автоматизированное сканирование Solar appScreener, среди iOS-версий исследованных приложений нет ни одного, удовлетворяющего хотя бы среднему по отрасли уровню защищенности. Приложение Mi FIT продемонстрировало наиболее низкий среди всех iOS-версий результат общего уровня защищенности – 0.0 балла из 5.0

Ростелеком
Солар

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70