ПУТИ РЕШЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ

А.А. Герасимович

Белорусский государственный университет, г. Минск
cw145@mail.ru
науч. рук. – Е.А. Чудовская, канд. физ.-мат. наук, доц.

На сегодняшний день в мире большое количество удобных мобильных приложений, многие из которых не могут похвастаться высоким уровнем безопасности. В последнее время значительно возросло число успешных хакерских атак на пользовательские приложения. В результате таких атак похищаются не только огромные денежные средства, но и пользовательские данные. Это связано с тем, что современные приложения имеют массу уязвимостей разной степени риска: уязвимости только высокого риска были обнаружены в 38 % мобильных приложений для iOS и в 43 % приложений для Android. Большинство проблем с безопасностью встречается на обеих платформах. Небезопасное хранение данных – самая распространенная проблема, встречающаяся в 76 % мобильных приложений. Под угрозой находятся пароли, финансовая информация, личные данные и переписка. Большинство случаев вызвано слабостью механизмов безопасности (74 % и 57 % для приложений iOS и Android соответственно и 42% для серверных компонентов). В данной работе описывается недавно обнаруженная уязвимость в операционной системе Android, ее суть, проблематика и возможный способ решения. Ценность работы заключается в смещении приоритетов при разработке в сторону подхода, ориентированного на безопасность приложений. Множество уязвимостей, которые используют злоумышленники, уже известны, но недостаточно изучены, следовательно, в них необходимо разобраться.

Ключевые слова: Android, уязвимость, StrandHogg, безопасность.

ВВЕДЕНИЕ

На сегодняшний день количество устройств, работающих на операционной системе Android, превышает 2,5 миллиарда единиц [1] и это число с каждым годом растет. Такое количество обусловлено ценовой доступностью устройств, легкостью разработки под данную операционную систему, интуитивностью ее использования. Однако, такое широкое распространение приводит к тому, что злоумышленники стремятся воспользоваться уязвимостями системы и атаковать как можно больше пользователей. Об одной из таких уязвимостей и пойдет речь.

УЯЗВИМОСТЬ STRANDHOGG

Исследователи в сфере безопасности ОС Android нашли [2] доказательства существования чрезвычайно опасной уязвимости, позволяющей

вредоносным приложениям притворяться обычными приложениями, в то время, как пользователи даже не подозревают, что они атакованы.

ЗОНА РИСКА

Абсолютно все версии ОС Android;
практически все популярные приложения Google Play Market.

УГРОЗЫ

- Прослушивание пользователя через микрофон его устройства;
- фото и видео съемка с использованием камеры устройства;
- чтение и отправка SMS-сообщений;
- возможность удалённо совершать звонки пользователя;
- кража личных данных авторизации;

Всего специалистами было обнаружено 36 вредоносных приложений, использующих данную уязвимость. Среди них были разновидности так называемого BankBot [3] - банковского вируса, активно используемого в 2017 году. Во время тестирования было выявлено, что все самые популярные приложения уязвимы подобного рода атаке. Все версии ОС Android подвержены риску.

СПОСОБ ПОЛУЧЕНИЯ ДОСТУПА

Уязвимость позволяет вредоносному приложению запрашивать разрешения, притворяясь другим, совершенно безвредным приложением. Это могут быть любые разрешения, включая доступ к SMS, фото, микрофону, GPS. Все эти разрешения позволяют читать сообщения, просматривать фотографии, записывать речь и контролировать передвижения ничего не подозревающего пользователя.

Суть атаки заключается в запросе разрешений, не вызывающих подозрений, будучи запрашиваемыми тем приложением, которому пользователь доверяет. Человек, не подозревающий об атаке, дает эти разрешения приложению, притворяющемуся приложением, которое пользователь хочет открыть.

Используя данную уязвимость, установленное вредоносное приложение может атаковать устройство следующим образом: когда пользователь нажимает на иконку нужного ему безвредного приложения, вместо него открывается вредоносное приложение, заменяющее интерфейс ориги-

нала. После ввода данных при логине или регистрации, информация моментально отправляется злоумышленнику, который получает доступ к аккаунту и может им управлять.

ОБЪЯСНЕНИЕ УЯЗВИМОСТИ

Проблема заключается в уязвимости системы мультизадачности ОС Android, позволяющая одним приложениям маскироваться под другие. Эта уязвимость основана на настройке управления Android под названием «taskAffinity» [4], которая позволяет любому приложению, в том числе вредоносному, свободно использовать любую личность в желаемой многозадачной системе.

Описанная выше уязвимость работает, когда вредоносное приложение устанавливает флаг taskAffinity для одного или нескольких своих действий в соответствии с packageName любого стороннего приложения. Затем, либо в сочетании с allowTaskReparenting = "true" в манифесте, либо путем запуска активности с флагом FLAG_ACTIVITY_NEW_TASK [5], вредоносная активность будет размещена внутри задачи жертвы и поверх нее.

Таким образом, вредоносная активность захватывает задачу цели. В следующий раз, когда целевое приложение будет запущено из меню, захваченная задача будет выведена на передний план, и вредоносная активность будет видна. В этом случае вредоносное приложение должно выглядеть как целевое приложение, чтобы успешно запускать атаки против пользователя.

МАСКИРОВКА АТАКИ

Уязвимость сосредоточена на активностях и их перемещениях между задачами в системе многозадачности Android. При запуске двух или более мероприятий одновременно с функцией startActivities (android.content.Intent[]), вредоносное приложение может начать атаку и «стать» приложением, которое кажется невиновным.

Если взглянуть на выходные данные активностей, видно, что атакующая активность уже на месте и скрывается до следующего запуска приложения. И действительно, при следующем запуске приложения-жертвы, пользователь увидит атакующее приложение вместо приложения-жертвы.

МОНИТОРИНГ ЗАДАЧ

Злоумышленник может получить значительный контроль над задачей жертвы. Комбинируя с намерениями FLAG_ACTIVITY_NEW_TASK [5]

и FLAG_ACTIVITY_CLEAR_TASK [5], злоумышленник сначала очищает целевую задачу, а затем попадает в нее. Далее он может завершить целевую задачу с помощью finishAndRemoveTask и запустить новую задачу с той же привязкой к FLAG_ACTIVITY_NEW_TASK [5] и FLAG_ACTIVITY_MULTIPLE_TASK [5] и, таким образом, создать новую целевую задачу, которая гарантированно будет под контролем злоумышленника. После этого он может запустить фактическую активность программы жертвы и позволить приложению жертвы работать в обычном режиме, что нейтрализует у пользователя любые подозрения о взломе.

СПОСОБЫ ПРЕДОТВРАЩЕНИЯ УЯЗВИМОСТИ

- Внимательность пользователя;
- наличие антивирусного ПО;
- установка приложений только из официальных источников;
- установка разработчиком ПО привязки к задаче на «» (пустая строка) для всех активностей его приложения.

Однако важно уточнить, что вышеперечисленные способы лишь частично снижают риск.

Хотелось бы отметить важность построения мощной и качественной безопасности в приложениях. Реализация такого уровня безопасности лежит целиком и полностью на плечах разработчиков, которые зачастую думают о красоте, функицональности и доходах, нежели о защищенности их приложений, что зачастую приводит к катастрофическим последствиям как для их пользователей, так и для авторитета их компаний. Современный подход требует обратной расстановки приоритетов, в котором на первом месте будет стоять вопрос безопасности мобильных приложений и устройств.

ЗАКЛЮЧЕНИЕ

На сегодняшний день в операционной системе Android по-прежнему остаются подобные уязвимости, с которыми работают специалисты по безопасности и разработчики Google. И несмотря на то, что у большинства из этих уязвимостей уже есть способы их решения, все еще остаются те, которыми продолжают пользоваться злоумышленники. И это не говоря о тех уязвимостях, которые ждут своего времени, чтобы быть обнаруженными и использованными. Задача разработчиков остается в предусмотрении всех возможных способов защиты, а рядовых пользователей – во внимательности и аккуратности при использовании своих Android-устройств.

Библиографические ссылки

1. Статистика Android-устройств в мире [Электронный ресурс]. URL: https://www.ixbt.com/news/2019/05/08/2-5-google-android.html (дата обращения: 24.03.2021).
2. The StrandHogg Vulnerability [Электронный ресурс]. URL: https://promon.co/security-news/strandhogg/ (дата обращения: 25.03.2021).
3. Банкер Android.BankBot.149 стал грозным оружием киберпреступников [Электронный ресурс]. URL: https://news.drweb.ru/show/?i=11772&lng=ru (дата обращения: 25.03.2021).
4. Android Developers Activity [Электронный ресурс]. URL: https://developer.android.com/guide/topics/manifest/activity-element (дата обращения: 28.03.2021).
5. Android Developers Intent [Электронный ресурс]. URL: https://developer.android.com/reference/android/content/Intent (дата обращения: 28.03.2021).