Краткий обзор решения

Защита от уязвимостей реализации SSL на мобильных устройствах

Сегодня, когда существуют мобильные приложения для выполнения практически любой задачи, а каждая новаторская идея разработчиков встречается с большим энтузиазмом, пользователи редко задумываются о том, что использование мобильных приложений, уязвимых для атак типа «незаконный посредник» (man in the middle), может привести к раскрытию конфиденциальной информации и, как следствие, к подрыву доверия к приложениям, которые вообще-то считаются безопасными. Разработчики мобильных приложений тоже легкомысленно относятся к проблеме обеспечения конфиденциальности и безопасности пользователей. Тем не менее, именно разработчики обязаны обеспечить защиту частной информации пользователей своих приложений от уязвимостей в протоколах шифрования. Речь идет о таких уязвимостях, как BERserk, Heartbleed и т. д. (их перечень постоянно увеличивается).

В сентябре 2014 года CERT, первая группа быстрого реагирования на нарушения компьютерной безопасности при Университете Карнеги — Меллон, опубликовала список мобильных приложений, уязвимых для атак типа «незаконный посредник». Уязвимость этих приложений заключается в том, что они некорректно проверяют подлинность сертификатов SSL, подвергая имена пользователей и пароли риску раскрытия в ходе возможных атак.[1] Спустя пять месяцев, в январе 2015 года, специалисты McAfee® Labs обнаружили, что в 18 из 25 самых популярных приложений этого списка данная уязвимость до сих пор не устранена, при том что некорректная проверка цепочки цифровых сертификатов является одной из самых простых уязвимостей SSL.

Поскольку разработчики мобильных приложений, как мы видим, не справляются с растущим спросом на более высокий уровень конфиденциальности и безопасности, пользователям и предприятиям необходимо взять на вооружение все доступные средства, позволяющие обеспечить максимальную безопасность мобильных приложений.

Как защититься от уязвимостей в мобильных приложениях

Вот несколько рекомендаций по защите от опасностей, исходящих от уязвимых мобильных приложений:

- Загружайте и устанавливайте только такие приложения, которые хорошо известны, имеют высокий рейтинг и происходят из доверенных источников.
- Создавайте учетные записи только в том случае, если это позволяет получить значительные преимущества, недоступные временным пользователям («гостям»). Для каждой учетной записи создавайте уникальный пароль.

intel Security

- Регулярно тестируйте мобильные приложения, используемые в корпоративной среде, на наличие в них уязвимостей, чтобы не подвергать конфиденциальную информации риску раскрытия.
- Перед загрузкой мобильных приложений знакомьтесь с их политиками конфиденциальности, чтобы знать, к каким данным (информация о местоположении, доступ к вашим социальным сетям) могут получать доступ эти приложения на устройствах пользователя и как эти данные используются.

Как защититься от уязвимостей в мобильных приложениях с помощью Intel Security

McAfee VirusScan® Mobile

McAfee VirusScan Mobile — это система защиты от вредоносного программного обеспечения, которая осуществляет сканирование и очистку данных в мобильных средах с целью предотвращения ущерба, наносимого вирусами, троянами и другими вредоносными программами. McAfee VirusScan Mobile защищает ваши мобильные устройства в самых уязвимых точках, к которым относятся входящие и исходящие электронные письма, текстовые сообщения, приложения к электронным письмам и загрузки из сети Интернет.

- **Мгновенное обнаружение угроз.** Мгновенное блокирование вредоносных программ в электронных письмах, текстовых сообщениях и приложениях к электронным письмам. McAfee VirusScan Mobile обеспечивает автоматическую всестороннюю защиту смартфонов, проводя проверку на наличие целого ряда вредоносных программ менее чем за 200 миллисекунд.
- **Конфиденциальность приложений.** Вы можете видеть, к какой информации личного характера имеют доступ установленные вами приложения. Это позволяет обеспечить защиту такой информации и избавиться от ненужных рисков раскрытия данных.
- **Снижение риска, связанного с уязвимостями в SSL.** Когда приложения посылают конфиденциальную информацию, используя уязвимые соединения, McAfee VirusScan Mobile рассылает уведомления об угрозах. Уязвимые приложения он классифицирует как потенциально нежелательные программы (ПНП).

Комплекты McAfee Complete Endpoint Protection

Комплекты **McAfee Complete Endpoint Protection** полностью интегрируются с получившим признание специалистов программным обеспечением **McAfee® ePolicy Orchestrator® (McAfee ePO™)** для управления средствами защиты. Комплекты McAfee Complete Endpoint Protection и программное обеспечение McAfee ePO дают предприятиям возможность управлять мобильными пользователями и защищать их от мобильных вредоносных программ, риска утечки данных и других угроз.

- **Централизованно управляемые средства антивирусной защиты и проверки репутации приложений.** Они автоматически находят информацию, позволяющую оценивать репутацию приложений, а также быстро проверяют приложения на наличие целого ряда вредоносных угроз (одна проверка занимает менее 200 миллисекунд), обеспечивая тем самым автоматическую и комплексную защиту смартфонов.
- **Вся информация в одном окне.** McAfee ePO дает возможность управлять как средствами защиты смартфонов под управлением Google Android, Apple iOS и Microsoft Windows, так и средствами защиты традиционных конечных точек, обеспечивая автоматизированное развертывание и применение политик независимо от устройства и конечной точки.

- **Применение политик.** Эти комплекты позволяют блокировать доступ к корпоративной электронной почте при обнаружении на устройствах пользователей вредоносных программ или ПНП. Кроме того, средства автоматизации McAfee ePO позволяют выполнять с устройствами и другие действия (например, удалять все данные с устройства, переносить устройство в новую область системного дерева, в которой всем устройствам отказано в доступе к корпоративной VPN, и т. п.).

Intel Security True Key

Технология **True Key**, разработанная специалистами Intel Security, представляет собой простой и безопасный способ входа в приложения на мобильных телефонах. Она избавляет пользователей от необходимости запоминать пароли и дает им возможность мгновенно осуществлять вход в приложения, сайты и устройства, используя разные уникальные факторы проверки подлинности.

- **Распознавание лица вместо пароля.** Для входа можно использовать такие уникальные идентификаторы пользователя, как пропорции лица (расстояние между глазами и носом) или другие принадлежащие пользователю устройства.
- **Упрощение процесса создания и хранения уникальных паролей.** True Key сохраняет пароли и мгновенно осуществляет вход пользователя в веб-сайты и приложения, поэтому пользователям не нужно помнить несколько разных паролей.
- **Многофакторная идентификация.** Для повышения уровня своей безопасности пользователи могут использовать несколько разных уникальных факторов. Чем больше факторов используется, тем надежнее защита.

Защитив своих мобильных сотрудников от плохо реализованных приложений, вы избавитесь от ненужных рисков раскрытия конфиденциальной информации своей компании. Технологии Intel Security помогут вашей компании обеспечить упреждающую защиту от уязвимостей, подрывающих традиционную модель доверия.

1. **http://www.kb.cert.org/vuls/id/582497**

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com