Беспроводные KRACK нападают на обходной путь клиентской стороны и обнаружение

Содержание

Введение

16 октября ряд уязвимостей, широко известных как KRACK влияние на другие протоколы, используемые в сетях WiFi, был обнародован. Они влияют на протоколы безопасности, используемые в сетях WPA/WPA2, которые могли поставить под угрозу конфиденциальность данных или целостность, когда это передано по беспроводному соединению.

Практический уровень влияния варьируется значительно на каждом сценарии, плюс не, на все реализации клиентской стороны влияют таким же образом.
Атаки используют другие умные сценарии “проверки отрицательных состояний”, где изменения состояния, не должным образом определенные на стандартах беспроводной связи, пробует, и в большинстве случаев, не обрабатывает должным образом устройство, на которое влияют. Это не против алгоритмов шифрования, используемых для защиты WPA2, а о том, как аутентификация и согласования протокола сделаны во время обеспечения беспроводного соединения.

О большинстве сценариев уязвимостей сообщили для клиентов, где возможная типичная атака будет использовать поддельный Aps в качестве “человека в середине”, чтобы перехватить и ввести определенные кадры во время согласований безопасности между клиентом и реальным AP (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081). Это фокус этого документа

Один сценарий был описан, напав на инфраструктуры AP, которые предоставляют 802.11r (фут) быстрые услуги роуминга (CVE-2017-1382), который закреплен на недавно освобожденном коде AireOS

Существует 4 остающихся атаки на клиентские определенные протоколы: STK, TDLS, WNM, которые непосредственно не поддерживаются инфраструктурой AireOS (CVE-2017-13084

CVE-2017-13086 CVE-2017-13087 CVE-2017-13088) и выходят за рамки этого документа

На практике атакующий мог дешифровать трафик для сеанса, на который влияют или ввести кадры в одном или двух направлениях. Это не предоставляет способ декодировать ранее существующий трафик до атаки, ни это предоставит механизм для “получения” шифрования kays всех устройств в данном SSID или их PSK или паролях 802.1x

Уязвимости являются real и оказывают значительное влияние, но они не означают, что на защищенные сети WPA2 “влияют навсегда”, поскольку проблема может быть устранена путем улучшения реализаций и на клиенте и на стороне AP, для работы должным образом в тех *отрицательных сценариях проверки*, которые в настоящее время не обрабатываются устойчивым способом

Что должно клиент делать:

- Для уязвимостей стороны AP: Обновление является рекомендуемым действием при использовании FT. если FT не необходим для голоса/видеосервисов, оцените, если опция FT должна быть отключена, пока обновление к фиксированной длине кодового не сделано. При использовании голоса оцените, если CCKM выполним (клиентская сторона должна поддержать), или обновление к фиксированной длине кодового. Если № FT/802.11r используется, нет никакой потребности обновить в это время
- Для уязвимостей клиентской стороны улучшите свою видимость: гарантируйте, что постороннее обнаружение включено, покрыв все каналы и правило сообщить “об управляемом SSID”, поскольку злонамеренный создан. Кроме того, внедрите изменения конфигураций повторной попытки EAPoL, которые могут ограничить или полностью заблокировать атаки, которые будут выполнены, как описано в этом docuemnt

Основные ссылочные информационные сообщения в https://программные средства. cisco . com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Используемые компоненты

Внимание этого документа на Контроллеры беспроводной локальной сети, работающие, освобождает 8.0 или позже.

Требования

Знание содержания, покрытого упомянутой выше рекомендацией по вопросам безопасности, требуется.

Для WPA атаки KRACK существует 2 основных действия, которые мы можем взять для защиты клиентов, которые еще не были исправлены.

1. EAPoL (EAP по LAN) повторяют защиту

2. Постороннее обнаружение и функции олицетворения Точки доступа (AP), чтобы обнаружить, если используются инструменты атаки

Меры защиты Атаки EAPoL

Для vulnerabilities-2017-13077 к 81, относительно легко предотвратить клиентов, чтобы влияться, с помощью обнуленного счетчика повторов EAPoL. Эта конфигурация доступна во всех версиях WLC

Почему это работает

Для атаки нужна в минимуме одна дополнительная повторная попытка EAPoL, генерируемая средством проверки подлинности во время 4 этапных установлений связи, или во время ротации (широковещательных) ключей. Если мы блокируем генерацию повторных попыток, атака не может быть применена против Попарного переходного ключа (PTK)/Groupwise Переходный Ключ (GTK).

Возможное влияние

1. Клиенты, которые являются медленными или могут отбросить начальную обработку EAPoL M1 (т.е. первое сообщение 4 путей обмен ключами). Это замечено на некоторых маленьких клиентах или некоторых телефонах, которые могут получить M1 и не быть готовы обработать его после того, как фаза проверки подлинности dot1x, или сделать это также замедляются для совещания короткого таймера повторной передачи

2. Сценарии с плохой средой RF или подключения к глобальной сети (WAN) между AP и WLC, который может вызвать отбрасывание пакета в некоторый момент на передаче к клиенту.

В обоих сценариях результат был бы то, что о сбое обмена EAPoL можно сообщить, и клиент будет deauthenticated, он должен будет перезапустить ассоциацию и процессы проверки подлинности.

Для уменьшения вероятности несения в эту проблему более длинный таймаут должен использоваться (1000 мс), чтобы позволить большему количеству времени для медленных клиентов отвечать. По умолчанию составляет 1000 мс, но, возможно, был изменен на минимальное значение вручную, таким образом, он должен быть проверен.

!--- конфигурацию

Существует два механизма, доступные для настройки этого изменения.

- Глобальный, доступный во всех версиях
- На WLAN, доступный от 7.6 до последнего

Глобальная опция более проста, и может быть сделана во всех версиях, влияние через все WLAN в WLC.

На конфигурацию WLAN установка позволяет более тонкую настройку с возможностью ограничить, на какой SSID влияют, таким образом, изменения могли быть применены типы для каждого устройства, и т.д., если они сгруппированы на определенном vlans. Это доступно от версии 7.6

Например, это могло быть применено к WLAN 802.1x общего назначения, но не в голос определенный WLAN, где это может оказать большее влияние

Глобальная конфигурация #1:

```
config advanced eap eapol-key-retries 0
```

(CLI только опция)

Значение может быть проверено с:

```
(2500-1-ipv6) >show advanced eap

EAP-Identity-Request Timeout (seconds)..... 30

EAP-Identity-Request Max Retries.............. 2

EAP Key-Index for Dynamic WEP................. 0

EAP Max-Login Ignore Identity Response..... enable

EAP-Request Timeout (seconds)................. 30

EAP-Request Max Retries....................... 2

EAPOL-Key Timeout (milliseconds)............... 1000

EAPOL-Key Max Retries......................... 0

EAP-Broadcast Key Interval..................... 3600
```

#2 на Config WLAN

ID X=WLAN

```
config wlan security eap-params enable X

config wlan security eap-params eapol-key-retries 0 X
```

Если клиент удален должный обнулить повторные передачи, как определить

Клиент был бы удален из-за Max. повторных попыток EAPoL, достигнутых, и deauthenticated. Количество retransmit равняется 1, поскольку посчитан исходный кадр

```
 *Dot1x_NW_MsgTask_6: Oct 19 12:44:13.524: 28:34:a2:82:41:f6 Sending EAPOL-Key Message to mobile
28:34:a2:82:41:f6
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
..
*osapiBsnTimer: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 802.1x 'timeoutEvt' Timer expired for
station 28:34:a2:82:41:f6 and for message = M3
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 Retransmit failure for EAPOL-Key M3
to mobile 28:34:a2:82:41:f6, retransmit count 1, mscb deauth count 0
..
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.043: 28:34:a2:82:41:f6 Sent Deauthenticate to mobile on
BSSID 58:ac:78:89:b4:19 slot 1(caller 1x_ptsm.c:602)
```

Постороннее обнаружение

> Несколько из способов атаки для уязвимостей против клиентского шифрования PMK/GTK, должен “предоставить” поддельному AP тот же SSID как AP инфраструктуры, но воздействующий на другой канал. Это может быть легко обнаружено, и администратор сети может принять физические меры на основе его, поскольку это - видимое действие.

Существует 2 пути, предложенные до сих пор, чтобы сделать атаки EAPoL:

- Фальсифицирование AP инфраструктуры, другими словами, действие как посторонний AP, использование того же мак адреса, реального AP, но на другом канале. Легкий сделать для атакующего, но видимый
- Введение кадров в допустимое соединение, принуждение клиента реагировать. Это намного менее видимо, но обнаруживаемо при некоторых условиях, этому, возможно, понадобится очень тщательная синхронизация, чтобы быть успешным

Если "поддельное AP" размещается в сеть, комбинация функций олицетворения AP и постороннего обнаружения может обнаружить.

!--- конфигурацию

- Проверьте то постороннее обнаружение, включен на точках доступа. Это включено по умолчанию, но, возможно, было отключено вручную admin, таким образом, он должен быть проверен.
- Создайте правило отметить использование жуликов, “управлял SSIDs” как злонамеренным:
- Гарантируйте, что мониторинг канала установлен во “все каналы” для обоих 802.11a/b сети. Основная атака разработана, чтобы быть рядом с точки зрения RF, клиента, на другом канале от того, что используется на AP инфраструктуры. Это - то, почему важно гарантировать, что просмотрены все возможные каналы:

Олицетворение AP

Если инструмент атаки использует один из наших мак адресов AP, на конфигурации по умолчанию инфраструктура может обнаружить. Об этом сообщают как trap-сообщение SNMP и было бы индикацией, что атака имеет место.

```
Impersonation of AP with Base Radio MAC bc:16:65:13:a0:40 using source address of
bc:16:65:13:a0:40 has been detected by the AP with MAC Address: bc:16:65:13:a0:40 on its
802.11b/g radio whose slot ID is 0
```

Ссылки

Предупреждение рекомендации по вопросам безопасности

Посторонний менеджмент в Unified Wireless Network с помощью v7.4 - Cisco

Оптимальные методы конфигурации контроллера беспроводной локальной сети Cisco - Cisco

Постороннее обнаружение под Unified Wireless Network - Cisco