Solución alternativa y detección del lado del cliente del ataque de la Tecnología inalámbrica KRACK

Contenido

Introducción

En octubre 16, un conjunto de las vulnerabilidades conocidas extensamente como KRACK que afectaba a diversos protocolos usados en las redes de WiFi se han hecho públicos. Afectan a los protocolos de Seguridad usados en WPA/WPA2 las redes, que podrían comprometer la privacidad de los datos o la integridad cuando se transmiten sobre una conexión de red inalámbrica.

El nivel práctico de impacto varía perceptiblemente en cada escenario, más no todo el lado del cliente que las implementaciones se afectan en la misma manera.
Los ataques utilizan diversos escenarios listos de la “prueba negativa” donde las transiciones de estado definidas no correctamente en los estándares inalámbricos se intentan, y en la mayoría de los casos, no dirigido correctamente por el dispositivo afectado. Está no contra los algoritmos de cifrado usados para proteger el WPA2, sino en cómo la autenticación y las negociaciones del protocolo se hacen durante la sujeción de la conexión de red inalámbrica.

La mayor parte de los escenarios de las vulnerabilidades han estado señalados para los clientes, donde el ataque típico posible utilizará los Aps falsos como “hombre en el centro” para interceptar y para inyectar las tramas específicas durante las negociaciones de seguridad entre el cliente y el AP real (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081). Éstos son el foco de este documento

Un escenario se ha descrito que atacaba las infraestructuras AP que proporcionan los servicios rápidos de itinerancia 802.11r (pie) (CVE-2017-1308), que se repara en el código recientemente liberado de AireOS

Hay 4 ataques restantes contra los protocolos específicos del cliente: STK, TDLS, WNM, que no

son soportados directamente por la infraestructura de AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088), y están fuera del ámbito de este documento

En la práctica, un atacante podría desencriptar el tráfico para la sesión afectada, o inyecte las tramas en uno o dos direcciones. no proporciona una manera de decodificar el tráfico previamente existente, antes del ataque, ni proporcionará un mecanismo “obtiene” los kays del cifrado de todos los dispositivos en un SSID dado o su PSK o contraseñas del 802.1x

El conjunto de las vulnerabilidades es real, y tiene un impacto significativo, pero no significan que las redes protegidas WPA2 “están afectadas para siempre”, mientras que el problema puede ser reparado mejorando las implementaciones en el cliente y el lado AP, para trabajar correctamente en esos *escenarios de prueba negativos* que no se manejen actualmente de una manera robusta

Qué debe un cliente hacer:

- Para las vulnerabilidades del lado AP: La actualización es la acción recomendada si usa el pie si el pie no es necesario para la Voz/los servicio de video, evalúa si se inhabilita la característica pie hasta que la actualización a la fija de código se haga. Si usa la Voz, evalúe si el CCKM es posible (el lado del cliente necesita soportar), o actualización a la fija de código. Si no hay FT/802.11r funcionando, no hay necesidad de actualizar ahora
- Para las vulnerabilidades del lado del cliente, mejore su visibilidad: asegúrese de que la detección del granuja esté habilitada, cubriendo todos los canales, y una regla para señalar el “SSID manejado” como malévolo se crea. Además, implemente los cambios de configuraciones de la recomprobación de EAPoL que pueden limitar o bloquean totalmente los ataques que se realizarán, según lo descrito en este documento

El advisory principal de la referencia está en https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Componentes usados

Este documento se centra en los reguladores inalámbricos que ejecutan las versiones 8.0 o más adelante.

Requisitos

El conocimiento del contenido cubierto por el Security Advisory mencionado anteriormente se requiere.

Para los ataques WPA KRACK, hay 2 acciones principales que podemos tomar para proteger a los clientes que no se han parcheado todavía.

1. Protección de la recomprobación de EAPoL (EAP sobre el LAN)

2. Detección rogue y características de la personificación del punto de acceso, detectar si se están utilizando las herramientas de ataque

Protecciones del ataque de EAPoL

Para vulnerabilities-2017-13077 a 81, es relativamente fácil prevenir a los clientes que se afectarán, usando un contador de reintentos de EAPoL fijado a cero. Esta configuración está disponible en todas las versiones del WLC

Porqué esto trabaja

Las necesidades del ataque en la recomprobación adicional de EAPoL del mínimo uno generada por el authenticator durante el way handshake 4, o durante la rotación de la clave del broadcast. Si bloqueamos la generación de recomprobaciones, el ataque no puede ser aplicado contra la clave transitoria en parejas transitoria de la clave (PTK) /Groupwise (GTK).

Impacto posible

1. Clientes que son lentos o pueden caer el proceso inicial de EAPoL M1 (es decir el primer mensaje del intercambio de claves de 4 maneras). Esto se ve en algunos pequeños clientes o algunos teléfonos, que pueden recibir el M1, y no estar listo para procesarlo después de la fase de autenticación del dot1x, o hágalo demasiado lento para resolver un temporizador de retransmisión corto

2. Escenarios con el mún entorno RF, o conexiones WAN entre el AP y el WLC, que pueden causar una caída de paquetes en algún momento en la transmisión hacia el cliente.

En ambos escenarios, el resultado sería que un error del intercambio de EAPoL puede ser señalado, y el cliente deauthenticated, tendrá que recomenzar la asociación y los procesos de autenticación.

Para bajar las probabilidades para este problema, un descanso más largo se debe utilizar (1000 milisegundos), para dar la hora para que los clientes lentos respondan. El valor por defecto es 1000msec, pero se habría podido cambiar a un valor inferior manualmente así que debe ser verificado.

Configuración

Hay dos mecanismos disponibles configurar este cambio.

- Global, disponible en todos versiones
- Por la red inalámbrica (WLAN), disponible desde 7.6 a la más último

La opción global es más simple, y se puede hacer en todas las versiones, el impacto está a través de todos los WLAN en el WLC.

Por el ajuste de la configuración de la red inalámbrica (WLAN) permite que un control más granular, con la posibilidad limite que el SSID consigue afectado, así que los cambios podrían ser aplicados por los tipos de dispositivo, el etc, si se agrupan en los wlans específicos. Ésta es disponible desde versión 7.6

Por ejemplo, podría ser aplicada a una red inalámbrica (WLAN) genérica del 802.1x, pero no en una red inalámbrica (WLAN) específica de la Voz, donde puede tener un impacto más grande

Configuración global #1:

```
config advanced eap eapol-key-retries 0
```
(Opción CLI solamente)

El valor se puede validar con:

```
(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 por los Config de la red inalámbrica (WLAN)

X=WLAN ID

```
config wlan security eap-params enable X

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

Cómo identificar si un cliente es borrado debido a las retransmisiones cero

El cliente sería borrado debido a las recomprobaciones máximas de EAPoL alcanzado, y deauthenticated. La cuenta de la retransmisión es 1, pues se cuenta la trama inicial

```
 *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)
```

Detección rogue

Varias de las técnicas del ataque para las vulnerabilidades contra el cifrado del cliente PMK/GTK, necesitan “presentar” una falsificación AP con el mismo SSID que la infraestructura AP, pero funcionamiento en un diverso canal. Esto puede ser detectada fácilmente y el administrador de la red puede tomar medidas físicas basadas en él, pues es una actividad visible.

Hay 2 maneras propuestas hasta ahora para hacer los ataques de EAPoL:

- Falsificando la infraestructura AP, es decir actuando como granuja AP, usando el mismo MAC address, de un AP real, pero en un diverso canal. Fácil hacer para el atacante pero visible
- Inyectando las tramas en una conexión válida, forzando al cliente a reaccionar. Esto es mucho menos visible, pero inferior perceptible algunas condiciones, puede necesitar la sincronización muy cuidadosa ser acertada

La combinación de características de la personificación AP y de detección rogue puede detectar si una "falsificación ap" se está colocando en la red.

Configuración

- Valide que la detección del granuja está habilitada en los Puntos de acceso. Esto se habilita por abandono, pero se habría podido inhabilitar manualmente por el admin, así que debe ser verificada.
- Cree la regla para señalar a los granujas por medio de una bandera que usan los "SSID manejados" como malévolos:
- Asegúrese de que la supervisión del canal esté fijada a "todos los canales" para ambas redes 802.11a/b. El ataque bajo se diseña para ser cerca de perspectiva RF, el cliente, en un diverso canal de qué se utiliza en la infraestructura AP. Esta es la razón por la cual es importante asegurarse de que todos los canales posibles están analizados:

Personificación AP

> En la configuración predeterminada, la infraestructura puede detectar si la herramienta de ataque está utilizando uno de nuestros direccionamientos del mac AP. Esto está señalada como SNMP trap y sería indicación que está ocurriendo el ataque

```
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
```

Referencias

Aviso de Security Advisory