Solución alternativa y detección del lado del cliente de ataque de KRACK inalámbrico

Contenido

Introducción

El 16 de octubre, se hizo público un conjunto de vulnerabilidades ampliamente conocidas como KRACK que afectan a diferentes protocolos usados en redes Wi-Fi. Afectan a los protocolos de seguridad utilizados en las redes WPA/WPA2, lo que podría poner en peligro la integridad o la privacidad de los datos cuando se transmiten a través de una conexión inalámbrica.

El nivel práctico de impacto varía significativamente en cada escenario, además no todas las implementaciones del lado del cliente se ven afectadas de la misma manera.
Los ataques utilizan diferentes escenarios inteligentes de "pruebas negativas" en los que se prueban las transiciones de estado no definidas correctamente en los estándares inalámbricos y, en la mayoría de los casos, el dispositivo afectado no las gestiona correctamente. No va en contra de los algoritmos criptográficos utilizados para proteger WPA2, sino de cómo se realizan las negociaciones de autenticación y protocolo durante la protección de la conexión inalámbrica.

La mayoría de los escenarios de vulnerabilidades han sido notificados para los clientes, donde el posible ataque típico utilizará Aps falsos como "hombre en el medio" para interceptar e inyectar tramas específicas durante las negociaciones de seguridad entre el cliente y el AP real (CVE-2017-13077, CVE-2017-13078, CVE-20 7-13079, CVE-2017-13080, CVE-2017-13081). Estos son los objetivos de este documento

Se ha descrito un escenario en el que se atacan las infraestructuras AP que proporcionan servicios de itinerancia rápida 802.11r (FT) (CVE-2017-1382), que se fija en el código AireOS recientemente publicado

Quedan 4 ataques contra los protocolos específicos del cliente: STK, TDLS, WNM, que no son compatibles directamente con la infraestructura de AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-133 88), y están fuera del alcance de este documento

En términos prácticos, un atacante podría descifrar el tráfico para la sesión afectada, o inyectar tramas en una o dos direcciones . No proporciona una manera de decodificar el tráfico existente antes del ataque, ni proporciona un mecanismo para "obtener" los kays de cifrado de todos los dispositivos en un SSID determinado o sus contraseñas PSK o 802.1x

Las vulnerabilidades son reales y tienen un impacto significativo, pero no significan que las redes protegidas por WPA2 se "vean afectadas para siempre", ya que el problema se puede solucionar mejorando las implementaciones tanto en el lado del cliente como en el del AP, para funcionar correctamente en aquellos *escenarios de prueba negativos* que actualmente no se manejan de forma robusta

¿Qué debe hacer un cliente?

- Para vulnerabilidades del lado AP: Actualizar es la acción recomendada si se utiliza FT. si no se necesita FT para los servicios de voz/vídeo, evalúe si la función FT debe desactivarse hasta que se realice la actualización al código fijo. Si utiliza voz, evalúe si CCKM es viable (el cliente necesita soporte) o actualice a código fijo. Si no se utiliza FT/802.11r, no es necesario actualizar en este momento
- Para las vulnerabilidades del lado del cliente, mejore su visibilidad: asegúrese de que la detección no autorizada esté habilitada, abarcando todos los canales, y de que se cree una regla para informar de "SSID administrado" como malicioso. Además, implemente cambios en las configuraciones de reintento de EAPoL que pueden limitar o bloquear por completo los ataques que se van a realizar, como se describe en este documento

El principal asesor de referencia se encuentra en https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Componentes Utilizados

Este documento se centra en los controladores inalámbricos que ejecutan las versiones 8.0 o posteriores.

Requirements

Es necesario conocer el contenido cubierto por el aviso de seguridad mencionado anteriormente.

Para los ataques WPA KRACK, hay dos acciones principales que podemos tomar para proteger a los clientes que aún no han sido corregidos.

1. Protección de reintentos EAPoL (EAP sobre LAN)

2. Funciones de suplantación de puntos de acceso (AP) y detección de acceso no autorizados para detectar si se están utilizando las herramientas de ataque

Protección de ataques EAPoL

Para las vulnerabilidades 2017-13077 a 81, es relativamente fácil evitar que los clientes se vean afectados, usando un contador de reintentos EAPoL establecido en cero. Esta configuración está disponible en todas las versiones de WLC

Por qué funciona

El ataque necesita como mínimo un reintento EAPoL adicional generado por el autenticador durante el intercambio de señales de 4 direcciones o durante la rotación de la clave de broadcast. Si bloqueamos la generación de reintentos, el ataque no se puede aplicar a la clave transitoria de par (PTK)/clave transitoria de grupo (GTK).

Posible impacto

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

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

En ambos escenarios, el resultado sería que se puede informar de una falla de intercambio EAPoL, y que el cliente será desautenticado, tendrá que reiniciar los procesos de asociación y autenticación.

Para reducir la probabilidad de incurrir en este problema, se debe utilizar un tiempo de espera más largo (1000 mseg), para permitir más tiempo para que los clientes lentos respondan. El valor predeterminado es 1000 ms, pero se podría haber cambiado manualmente a un valor inferior para que se pueda verificar.

Configuración

Hay dos mecanismos disponibles para configurar este cambio.

- Global, disponible en todas las versiones
- Por WLAN, disponible de 7.6 a la última

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

La configuración de la WLAN permite un control más granular, con la posibilidad de limitar qué SSID se ve afectado, de modo que los cambios se puedan aplicar por tipo de dispositivo, etc, si se agrupan en wlan específicas. Esto está disponible en la versión 7.6

Por ejemplo, podría aplicarse a una WLAN 802.1x genérica, pero no a una WLAN específica de voz, donde puede tener un impacto mayor

Nº 1 de configuración global:

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

(opción solo de CLI)

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
```

Nº 2 por configuración WLAN

X=ID de WLAN

```
config wlan security eap-params enable X

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

Cómo identificar si un cliente se elimina debido a retransmisiones cero

El cliente se eliminaría debido a que se alcanzaron los reintentos máximos de EAPoL y se desautenticó. El conteo de retransmisión es 1, ya que 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 de Rogue

Varias de las técnicas de ataque para las vulnerabilidades contra el cifrado PMK/GTK del cliente, necesitan "presentar" un AP falso con el mismo SSID que el AP de infraestructura, pero funcionando en un canal diferente. Esto se puede detectar fácilmente y el administrador de la red puede realizar acciones físicas basadas en él, ya que se trata de una actividad visible.

Hasta el momento se han propuesto 2 maneras de realizar los ataques de EAPoL :

- Falsa infraestructura AP, en otras palabras, actuando como AP rogue, usando la misma dirección

mac, de un AP real, pero en un canal diferente. Fácil de hacer para el atacante pero visible
- Inyectar tramas en una conexión válida, obligando al cliente a reaccionar. Esto es mucho menos visible, pero detectable en algunas condiciones, puede ser necesario un tiempo muy cuidadoso para tener éxito

La combinación de las funciones de suplantación de AP y la detección de rogue puede detectar si se está colocando un "mapa falso" en la red.

Configuración

- Valide que la detección no autorizada esté habilitada en los puntos de acceso. Esto está habilitado de forma predeterminada, pero el administrador podría haberla desactivado manualmente, por lo que se debe verificar.
- Cree una regla para marcar los indicadores mediante "SSID gestionados" como maliciosos:
- Asegúrese de que la supervisión del canal esté configurada en "todos los canales" para ambas redes 802.11a/b. El ataque base está diseñado para estar cerca desde la perspectiva de RF, el cliente, en un canal diferente de lo que se utiliza en los AP de infraestructura. Por este motivo es importante asegurarse de que se analicen todos los canales posibles:

Suplantación de AP

En la configuración predeterminada, la infraestructura puede detectar si la herramienta de ataque está usando una de nuestras direcciones MAC AP. Esto se informa como una trampa SNMP y sería una indicación de que el ataque está ocurriendo.

```
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 aviso de seguridad

Gestión no autorizada en una red inalámbrica unificada con v7.4 - Cisco

Prácticas recomendadas de configuración del controlador de LAN inalámbrica de Cisco - Cisco

Detección no autorizada en Redes inalámbricas Unificadas - Cisco