Ação alternativa e detecção do lado do cliente do ataque do Sem fio KRACK

Índice

Introdução

Em outubro 16, um grupo de vulnerabilidades de conhecimento geral como KRACK que afeta os protocolos diferentes usados em redes de WiFi foram feitos públicos. Afetam os protocolos de segurança usados nas redes WPA/WPA2, que poderiam comprometer a privacidade de dados ou a integridade quando são transmitidas sobre uma conexão Wireless.

O nível prático do impacto varia significativamente em cada encenação, mais não todo o lado que do cliente as aplicações são afetadas da mesma forma.
Os ataques usam encenações inteligentes diferentes do “teste negativo” onde as transições de estado definidas não corretamente nos padrões wireless são tentadas, e na maioria dos casos, não segurado corretamente pelo dispositivo afetado. Está não contra os algoritmos de criptografia usados para proteger o WPA2, mas em como a autenticação e as negociações de protocolo são feitas durante a fixação da conexão Wireless.

A maioria das encenações das vulnerabilidades foram relatadas para os clientes, onde o ataque típico possível usará Aps falsificados como o “homem no meio” para interceptar e injetar quadros específicos durante as negociações de segurança entre o cliente e o AP real (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081). Estes são o foco deste documento

Uma encenação foi descrita que ataca as infra-estruturas AP que proporcionam (FT) os serviços 802.11r vagueando rápidos (CVE-2017-1382), que é fixado no código recentemente liberado de AireOS

Há 4 ataques permanecendo contra protocolos específicos do cliente: STK, TDLS, WNM, que não são apoiados diretamente pela infraestrutura de AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088), e são fora do âmbito deste documento

Na pr3tica, um atacante poderia decifrar o tráfego para a sessão afetada, ou injete quadros em um ou dois sentidos. Não fornece uma maneira de descodificar tráfego previamente existente, antes do ataque, nem fornecerá um mecanismo “obtém” os kays da criptografia de todos os dispositivos em um SSID dado ou em suas senhas PSK ou de 802.1x

As vulnerabilidades são reais, e têm um impacto significativo, mas não significam que as redes protegidas WPA2 “estão afetadas para sempre”, enquanto a edição pode ser fixada melhorando as aplicações no cliente e no lado AP, para trabalhar corretamente naqueles *cenários de teste negativos* que não são segurados atualmente em uma maneira robusta

O que deve um cliente fazer:

- Para vulnerabilidades do lado AP: A elevação é a ação recomendada se usando o FT. se o FT não é precisado para a Voz/serviços de vídeo, avalie se a característica FT for desabilitada até que a elevação ao código fixo esteja feita. Se usando a Voz, avalie se o CCKM é praticável (o lado do cliente precisa de apoiar), ou elevação ao código fixo. Se nenhum FT/802.11r está no uso, não há nenhuma necessidade de promover neste tempo
- Para vulnerabilidades do lado do cliente, melhore sua visibilidade: assegure-se de que a detecção do rogue esteja permitida, cobrindo todos os canais, e uma regra para relatar “o SSID controlado” como malicioso é criado. Adicionalmente, mudanças de configurações da nova tentativa de EAPoL do implementar que podem limitar ou obstruem inteiramente os ataques a ser executados, como descrito neste documento

O advisory principal da referência está em https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Componentes usados

Este documento focaliza nos controladores wireless que executam as liberações 8.0 ou mais atrasado.

Requisitos

O conhecimento do índice coberto pela Recomendação de Segurança mencionada acima é exigido.

Para os ataques WPA KRACK, há 2 ações principal que nós podemos tomar para proteger os clientes que não foram remendados ainda.

1. Proteção da nova tentativa de EAPoL (EAP sobre o LAN)

2. Detecção desonesto e de personificação do Access Point (AP) características, para detectar se as ferramentas de ataque estão sendo usadas

Proteções do ataque de EAPoL

Para vulnerabilities-2017-13077 a 81, é relativamente fácil impedir os clientes a ser afetados, usando um contador de nova tentativa de EAPoL ajustado a zero. Esta configuração está disponível em todas as versões WLC

Porque isto trabalha

O ataque precisa no mínimo uma nova tentativa adicional de EAPoL gerada pelo autenticador durante o reconhecimento de sentido 4, ou durante a rotação da chave da transmissão. Se nós obstruímos a geração de novas tentativas, o ataque não pode ser aplicado contra a chave transiente por pares transiente da chave (PTK) /Groupwise (GTK).

Impacto possível

1. Clientes que são lentos ou podem deixar cair o processamento inicial de EAPoL M1 (isto é a primeira mensagem das trocas de chave de 4 maneiras). Isto é visto em alguns clientes pequenos ou em alguns telefones, que podem receber o M1, e para não estar pronto para processá-lo após a fase de autenticação do dot1x, ou faça-o demasiado lento para encontrar um temporizador de retransmissões curto

2. Encenações com ambiente ruim RF, ou conexões de WAN entre o AP e o WLC, que podem causar uma queda de pacote de informação em algum momento na transmissão para o cliente.

Em ambas as encenações, o resultado seria que uma falha da troca de EAPoL pode ser relatada, e o cliente deauthenticated, terá que reiniciar a associação e os processos de autenticação.

Para diminuir a probabilidade de incorrer nesta edição, um intervalo mais longo deve ser usado (1000 milissegundos), para reservar mais hora para que os clientes lentos respondam. O padrão é 1000msec, mas poderia ter sido mudado a um valor mais baixo manualmente assim que deve ser verificada.

Configuração

Há dois mecanismos disponíveis para configurar esta mudança.

- Global, disponível em tudo libera-se
- Pelo WLAN, disponível de 7.6 ao mais tarde

A opção global é mais simples, e pode ser feita em todas as liberações, o impacto é através de todos os WLAN no WLC.

Pelo ajuste de configuração WLAN permite que um controle mais granulado, com a possibilidade limite que o SSID obtém impactado, assim que as mudanças poderiam ser aplicadas por tipos de dispositivo, etc., se são agrupadas em wlans específicos. Isto está disponível da versão 7.6

Por exemplo, poderia ser aplicado a um 802.1x genérico WLAN, mas não em uma Voz WLAN específico, onde pudesse ter um impacto maior

Config global #1:

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

(Opção CLI somente)

O valor pode ser validado com:

```
(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 pela configuração WLAN

X=WLAN ID

```
config wlan security eap-params enable X

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

Como identificar se um cliente é suprimido devido às retransmissões zero

O cliente seria suprimido devido às novas tentativas máximas de EAPoL alcançado, e deauthenticated. A contagem da retransmissão é 1, porque o frame inicial é contado

```
 *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)
```

Detecção desonesto

Diversas das técnicas do ataque para as vulnerabilidades contra a criptografia do cliente PMK/GTK, precisam “de apresentar” uma falsificação AP com o mesmo SSID que a infraestrutura AP, mas funcionamento em um canal diferente. Isto pode facilmente ser detectado e o administrador de rede pode tomar as ações físicas baseadas nele, porque é uma atividade visível.

Há 2 maneiras propostas até agora fazer os ataques de EAPoL:

- Falsificando a infraestrutura AP, ou seja atuando como o rogue AP, usando o mesmo MAC address, de um AP real, mas em um canal diferente. Fácil fazer para o atacante mas visível
- Injetando quadros em uma conexão válida, forçando o cliente a reagir. Isto é muito menos visível, mas inferior detectável algumas circunstâncias, pode precisar o sincronismo muito cuidadoso de ser bem

sucedido

A combinação de características da personificação AP e de detecção desonesto pode detectar se uma “falsificação ap” está sendo colocada na rede.

Configuração

- Valide que a detecção do rogue está permitida nos Access point. Isto é permitido à revelia, mas poderia ter sido desabilitado manualmente pelo admin, assim que deve ser verificada.
- Crie a regra para embandeirar rogues usando “SSID controlados” como maliciosos:
- Assegure-se de que a monitoração do canal esteja ajustada a “todos os canais” para ambas as redes 802.11a/b. O ataque baixo é projetado ser próximo da perspectiva RF, o cliente, em um canal diferente do que é usado na infraestrutura AP. Eis porque é importante assegurar-se de que todos os canais possíveis estejam feitos a varredura:

Personificação AP

Na configuração padrão, a infraestrutura pode detectar se a ferramenta de ataque está usando um de nossos endereços do Mac AP. Isto é relatado como uma armadilha de SNMP e seria indicação que o ataque está ocorrendo.

```
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
```

Referências

Observação de Recomendação de Segurança

Gerenciamento desonesto em uma rede Wireless unificada usando v7.4 - Cisco

Melhores prática da configuração do controlador de LAN do Cisco Wireless - Cisco

Detecção desonesto sob redes Wireless unificadas - Cisco