Solução alternativa e detecção do cliente de ataque KRACK sem fio

Contents

Introduction

No dia 16 de outubro, um conjunto de vulnerabilidades amplamente conhecidas como KRACK afetando diferentes protocolos usados em redes WiFi foi tornado público. Eles afetam os protocolos de segurança usados em redes WPA/WPA2, que podem comprometer a privacidade ou a integridade dos dados quando eles são transmitidos por uma conexão sem fio.

O nível prático de impacto varia significativamente em cada cenário, além de nem todas as implementações do lado do cliente serem afetadas da mesma forma.
Os ataques usam diferentes cenários inteligentes de "teste negativo", em que as transições de estado não adequadamente definidas nos padrões sem fio são testadas e, na maioria dos casos, não tratadas adequadamente pelo dispositivo afetado. Não é contra os algoritmos de criptografia usados para proteger a WPA2, mas sobre como as negociações de autenticação e protocolo são feitas durante a proteção da conexão sem fio.

A maioria dos cenários de vulnerabilidades foram relatados para clientes, onde o possível ataque típico usará Aps falsos como "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-201 7-13079, CVE-2017-13080, CVE-2017-13081). Estes são os pontos focais deste documento

Um cenário foi descrito atacando a infraestrutura de AP que fornece serviços de roaming rápido 802.11r (FT) (CVE-2017-1382), que é corrigido no código AireOS lançado recentemente

Há 4 ataques restantes contra protocolos específicos do cliente: STK, TDLS, WNM, que não são suportados diretamente pela infraestrutura AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-130 88) e estão fora do escopo deste documento

Em termos práticos, um invasor pode descriptografar o tráfego da sessão afetada ou injetar quadros em uma ou duas direções . Ele não fornece uma maneira de decodificar o tráfego existente anteriormente, antes do ataque, nem fornece um mecanismo para "obter" os kays de criptografia de todos os dispositivos em um SSID específico ou suas senhas PSK ou 802.1x

As vulnerabilidades são reais e têm um impacto significativo, mas não significam que as redes protegidas por WPA2 sejam "afetadas para sempre", já que o problema pode ser corrigido melhorando as implementações no lado do cliente e do AP, para funcionar adequadamente nos *cenários de teste negativos* que atualmente não são tratados de forma robusta

O que um cliente deve fazer:

- Para vulnerabilidades do lado AP: Atualizar é a ação recomendada se estiver usando o FT. se o FT não for necessário para serviços de voz/vídeo, avalie se o recurso FT deve ser desabilitado até que a atualização para código fixo seja feita. Se estiver usando voz, avalie se o CCKM é viável (o lado do cliente precisa suportar) ou atualize para código fixo. Se nenhum FT/802.11r estiver em uso, não há necessidade de atualização no momento
- Para vulnerabilidades do cliente, melhore sua visibilidade: certifique-se de que a detecção de invasores esteja ativada, abrangendo todos os canais, e uma regra para relatar "SSID gerenciado" quando for criado mal-intencionado. Além disso, implemente alterações nas configurações de repetição EAPoL que podem limitar ou bloquear totalmente os ataques a serem executados, conforme descrito neste documento

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

Componentes Utilizados

Este documento concentra-se nos Wireless Controllers que executam as versões 8.0 ou posterior.

Requirements

Énecessário o conhecimento do conteúdo coberto pela consultoria de segurança mencionada acima.

Para os ataques WPA KRACK, há duas ações principais que podemos tomar para proteger os clientes que ainda não foram corrigidos.

1. Proteção de repetição EAPoL (EAP sobre LAN)

2. Detecção de invasores e recursos de representação de ponto de acesso (AP), para detectar se as ferramentas de ataque estão sendo usadas

Proteções de ataque EAPoL

Para vulnerabilidades-2017-13077 a 81, é relativamente fácil evitar que os clientes sejam afetados, usando um contador de repetição EAPoL definido como zero. Essa configuração está disponível em todas as versões de WLC

Por que isso funciona

O ataque precisa de pelo menos uma nova tentativa EAPoL adicional gerada pelo autenticador durante o handshake de 4 vias ou durante a rotação da chave de broadcast. Se bloquearmos a geração de novas tentativas, o ataque não poderá ser aplicado contra Pairwise Transient Key (PTK)/Groupwise Transient Key (GTK).

Possível impacto

1. Clientes que estão lentos ou podem diminuir o processamento inicial do EAPoL M1 (ou seja, a primeira mensagem da troca de chaves de 4 vias). Isso é observado em alguns clientes pequenos ou em alguns telefones, que podem receber o M1, e não estão prontos para processá-lo após a fase de autenticação dot1x, ou que são lentos demais para atender a um temporizador de retransmissão curto

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

Em ambos os cenários, o resultado seria que uma falha de troca EAPoL pode ser relatada, e o cliente será desautenticado, ele terá que reiniciar os processos de associação e autenticação.

Para diminuir a probabilidade de ocorrência desse problema, deve ser usado um tempo limite mais longo (1000 ms), para permitir mais tempo para que os clientes lentos respondam. O padrão é 1000msec, mas pode ter sido alterado manualmente para um valor mais baixo para que seja verificado.

Configuração

Há dois mecanismos disponíveis para configurar essa alteração.

- Global, disponível em todas as versões
- Por WLAN, disponível da versão 7.6 para a mais recente

A opção global é mais simples e pode ser feita em todas as versões, o impacto ocorre em todas as WLANs na WLC.

Por configuração de WLAN permite um controle mais granular, com a possibilidade de limitar qual SSID é afetado, de modo que as alterações possam ser aplicadas por tipo de dispositivo, etc, se forem agrupadas em wlans específicas. Está disponível na versão 7.6

Por exemplo, ele pode ser aplicado a uma WLAN 802.1x genérica, mas não a uma WLAN específica para voz, onde pode ter um impacto maior

Nº 1 em configuração global:

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

(opção somente CLI)

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
```

Nº 2 por configuração de WLAN

X=ID da WLAN

```
config wlan security eap-params enable X

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

Como identificar se um cliente é excluído devido a retransmissões zero

O cliente seria excluído devido ao máximo de tentativas de EAPoL alcançadas e desautenticadas. A contagem de retransmissão é 1, à medida que o quadro 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 de invasores

Várias das técnicas de ataque para as vulnerabilidades contra a criptografia PMK/GTK do cliente precisam "apresentar" um AP falso com o mesmo SSID do AP de infraestrutura, mas operando em um canal diferente. Isso pode ser facilmente detectado e o administrador da rede pode executar ações físicas com base nele, pois é uma atividade visível.

Há duas maneiras propostas até o momento para fazer os ataques EAPoL:

- Falsificação de AP de infraestrutura, em outras palavras, atuar como AP invasor, usando o mesmo endereço MAC, de um AP real, mas em um canal diferente. Fácil de fazer pelo invasor, mas visível
- Injetando quadros em uma conexão válida, forçando o cliente a reagir. Isso é muito menos visível,

mas detectável sob algumas condições, pode precisar de um cronograma muito cuidadoso para ser bem-sucedido

A combinação de recursos de representação de AP e detecção de invasão pode detectar se um "ap falso" está sendo colocado na rede.

Configuração

- Confirme se a detecção de invasores está habilitada nos pontos de acesso. Isso é ativado por padrão, mas pode ter sido desabilitado manualmente pelo administrador, portanto, é necessário verificá-lo.
- Crie uma regra para sinalizar invasores usando "SSIDs gerenciados" como mal-intencionados:
- Certifique-se de que o monitoramento de canais esteja definido como "todos os canais" para ambas as redes 802.11a/b. O ataque básico foi projetado para estar próximo da perspectiva de RF, o cliente, em um canal diferente do usado nos APs de infraestrutura. É por isso que é importante garantir que todos os canais possíveis sejam verificados:

representação de AP

Na configuração padrão, a infraestrutura pode detectar se a ferramenta de ataque está usando um de nossos endereços MAC AP. Isso é relatado como uma armadilha SNMP e seria uma indicação de 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

Aviso de segurança

Gerenciamento invasor em uma rede sem fio unificada usando v7.4 - Cisco

Práticas recomendadas de configuração do Cisco Wireless LAN Controller - Cisco

Detecção de invasores em Unified Wireless Networks - Cisco