Solution de contournement et de détection des clients d'attaque sans fil KRACK

Contenu

Introduction

Le 16 octobre, un ensemble de vulnérabilités connues sous le nom de KRACK affectant différents protocoles utilisés dans les réseaux WiFi a été rendu public. Elles affectent les protocoles de sécurité utilisés sur les réseaux WPA/WPA2, ce qui peut compromettre la confidentialité ou l'intégrité des données lorsqu'elles sont transmises via une connexion sans fil.

Le niveau d'impact pratique varie considérablement selon chaque scénario, et toutes les mises en oeuvre côté client ne sont pas affectées de la même manière.
Les attaques utilisent différents scénarios intelligents de “ tests négatifs ” où les transitions d'état non correctement définies sur les normes sans fil sont essayées, et dans la plupart des cas, ne sont pas gérées correctement par le périphérique affecté. Il n'est pas opposé aux algorithmes de chiffrement utilisés pour protéger WPA2, mais à la manière dont l'authentification et les négociations de protocole sont effectuées lors de la sécurisation de la connexion sans fil.

La plupart des scénarios de vulnérabilités ont été signalés pour les clients, où l'attaque typique possible utilisera les faux Aps comme “ homme au milieu de la ” pour intercepter et injecter des trames spécifiques pendant les négociations de sécurité entre le client et le point d'accès réel (CVE-2017-13077, CVE-2017-13078, CVE-211117777 7-13079, CVE-2017-13080, CVE-2017-13081). Ces points sont au coeur de ce document

Un scénario a été décrit en attaquant l'infrastructure AP qui fournit des services d'itinérance rapide 802.11r (FT) (CVE-2017-1382), qui est corrigé sur le code AireOS récemment publié

Il reste 4 attaques contre des protocoles spécifiques aux clients : STK, TDLS, WNM, qui ne sont pas directement pris en charge par l'infrastructure AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13 88) et ne sont pas couverts par ce document

En termes pratiques, un pirate peut décrypter le trafic pour la session affectée, ou injecter des trames dans une ou deux directions. Il ne fournit pas un moyen de décoder le trafic existant précédemment, avant l'attaque, ni un mécanisme pour “ obtenir ” les clés de chiffrement de tous les périphériques d'un SSID donné ou de leurs mots de passe PSK ou 802.1x

Les vulnérabilités sont réelles et ont un impact significatif, mais elles ne signifient pas que les réseaux protégés par WPA2 sont “ affectés pour toujours ”, car le problème peut être résolu en améliorant les mises en oeuvre côté client et AP, pour fonctionner correctement dans les *scénarios de test négatifs* qui ne sont pas actuellement gérés de manière robuste

Que doit faire un client ?

- Pour les vulnérabilités côté AP : La mise à niveau est l'action recommandée si vous utilisez FT. si FT n'est pas nécessaire pour les services voix/vidéo, évaluez si la fonctionnalité FT doit être désactivée jusqu'à ce que la mise à niveau vers le code fixe soit effectuée. Si vous utilisez la voix, évaluez si CCKM est faisable (le côté client doit prendre en charge) ou effectuez une mise à niveau vers un code fixe. Si aucun FT/802.11r n'est utilisé, il n'est pas nécessaire de procéder à une mise à niveau pour le moment
- Pour les vulnérabilités côté client, améliorez votre visibilité : assurez-vous que la détection de virus est activée, couvrant tous les canaux, et qu'une règle pour signaler “ SSID géré ” malveillant est créée. En outre, implémenter des modifications de configuration des tentatives EAPoL qui peuvent limiter ou bloquer entièrement les attaques à effectuer, comme décrit dans ce document

Le principal avis de référence se trouve à https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Composants utilisés

Ce document se concentre sur les contrôleurs sans fil exécutant les versions 8.0 ou ultérieures.

Conditions requises

La connaissance du contenu couvert par l'avis de sécurité mentionné ci-dessus est requise.

Pour les attaques WPA KRACK, nous pouvons prendre deux mesures principales pour protéger les clients qui n'ont pas encore été corrigés.

1. Protection contre les tentatives EAPoL (EAP sur LAN)

2. Fonctions de détection des points d'accès et d'emprunt d'identité pour détecter si les outils d'attaque sont utilisés

Protection contre les attaques EAPoL

Pour les vulnérabilités-2017-13077 à 81, il est relativement facile d'empêcher les clients d'être affectés, à l'aide d'un compteur de tentatives EAPoL défini sur zéro. Cette configuration est disponible dans toutes les versions de WLC

Pourquoi ça marche

L'attaque nécessite au moins une nouvelle tentative EAPoL supplémentaire générée par l'authentificateur lors de la connexion en 4 étapes ou lors de la rotation de la clé de diffusion. Si nous bloquons la génération de nouvelles tentatives, l'attaque ne peut pas être appliquée contre PTK (Pairwise Transient Key)/GTK (Groupwise Transient Key).

Impact possible

1. Clients qui sont lents ou qui peuvent abandonner le traitement initial de EAPoL M1 (c'est-à-dire le premier message de l'échange de clés à 4 voies). Ceci est visible sur certains petits clients ou certains téléphones, qui peuvent recevoir le M1, et ne pas être prêt à le traiter après la phase d'authentification dot1x, ou le faire trop lentement pour répondre à un compteur de retransmission court

2. Scénarios avec un environnement RF incorrect, ou connexions WAN entre AP et WLC, qui peuvent provoquer une perte de paquet à un moment donné lors de la transmission vers le client.

Dans les deux scénarios, une défaillance d'échange EAPoL peut être signalée, et le client sera déauthentifié, il devra redémarrer les processus d'association et d'authentification.

Pour réduire la probabilité d'apparition de ce problème, il faut utiliser un délai d'attente plus long (1 000 ms), afin de laisser plus de temps aux clients lents pour répondre. La valeur par défaut est 1000msec, mais elle aurait pu être modifiée manuellement pour une valeur inférieure afin qu'elle soit vérifiée.

Configuration

Deux mécanismes sont disponibles pour configurer cette modification.

- Global, disponible dans toutes les versions
- Par WLAN, disponible de 7,6 à la version la plus récente

L'option globale est plus simple, et peut être effectuée dans toutes les versions, l'impact est sur tous les WLAN dans le WLC.

Le paramètre de configuration par WLAN permet un contrôle plus granulaire, avec la possibilité de limiter l'impact du SSID, afin que les modifications puissent être appliquées par type de périphérique, etc, si elles sont regroupées sur des WLAN spécifiques. Ceci est disponible à partir de la version 7.6

Par exemple, il peut être appliqué à un WLAN 802.1x générique, mais pas à un WLAN spécifique à la voix, où il peut avoir un impact plus important

Configuration globale n°1 :

```
config advanced eap eapol-key-retries 0
```
(option CLI uniquement)

La valeur peut être validée avec :

```
(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
```

N° 2 par configuration WLAN

X=ID WLAN

```
config wlan security eap-params enable X

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

Comment identifier si un client est supprimé en raison de zéro retransmission

Le client serait supprimé en raison de tentatives EAPoL maximales atteintes et déauthentifiées. Le nombre de retransmissions est égal à 1, car la trame initiale est comptée

```
 *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)
```

Détection de systèmes indésirables

Plusieurs des techniques d'attaque pour les vulnérabilités contre le cryptage PMK/GTK client, doivent “ présenter ” un faux AP avec le même SSID que l'AP d'infrastructure, mais fonctionnant sur un canal différent. Cela peut être facilement détecté et l’administrateur réseau peut effectuer des actions physiques en fonction de cela, car il s’agit d’une activité visible.

Il y a 2 façons proposées jusqu'à présent de faire les attaques EAPoL :

- Point d'accès d'infrastructure falsifié, en d'autres termes, agissant comme point d'accès non autorisé, utilisant la même adresse MAC, d'un point d'accès réel, mais sur un canal différent. Facile à faire pour

le pirate, mais visible

- Injection de trames dans une connexion valide, forçant le client à réagir. C'est beaucoup moins visible, mais détectable dans certaines conditions, il peut être nécessaire de choisir un timing très prudent pour réussir

La combinaison de fonctions d'emprunt d'identité AP et de détection de piratage peut détecter si un « faux point d'accès » est placé dans le réseau.

Configuration

- Validez que la détection des pirates est activée sur les points d'accès. Cette option est activée par défaut, mais elle aurait pu être désactivée manuellement par l'administrateur. Elle doit donc être vérifiée.
- Créez une règle pour marquer les rogues à l'aide de “ SSID gérés ” comme malveillants :
- Assurez-vous que la surveillance des canaux est configurée pour “ tous les canaux ” pour les deux réseaux 802.11a/b. L'attaque de base est conçue pour être proche du point de vue RF, du client, sur un canal différent de celui utilisé sur les points d'accès d'infrastructure. C'est pourquoi il est important de s'assurer que tous les canaux possibles sont analysés :

Emprunt d'identité AP

En configuration par défaut, l'infrastructure peut détecter si l'outil d'attaque utilise l'une de nos adresses MAC AP. Ceci est signalé comme un déroutement SNMP et indique que l'attaque est en cours.

```
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
```

Références

Avis de sécurité

Gestion des systèmes non fiables dans un réseau sans fil unifié utilisant la version 7.4 - Cisco

Meilleures pratiques de configuration du contrôleur de réseau local sans fil Cisco - Cisco

Détection des attaques sous Unified Wireless Networks - Cisco