Contournement et détection de côté client d'attaque de la radio KRACK

Contenu

Introduction

En octobre 16, un ensemble de vulnérabilités largement connues sous le nom de KRACK affectant différents protocoles utilisés dans des réseaux de WiFi ont été rendus publics. Ils affectent des protocoles de Sécurité utilisés sur les réseaux WPA/WPA2, qui pourraient compromettre la confidentialité des données ou l'intégrité quand ils sont transmis au-dessus d'une connexion Sans fil.

Le niveau pratique de l'incidence varie de manière significative sur chaque scénario, plus non tout le côté client que des réalisations sont affectées de la même manière.
Les attaques utilisent différents scénarios intelligents « du test négatif » où des transitions d'état pas correctement définies sur les normes sans fil sont essayées, et dans la plupart des cas, non manipulé correctement par le périphérique affecté. Il est non contre les cryptos algorithmes utilisés pour protéger le WPA2, mais sur la façon dont les négociations d'authentification et de protocole sont faites pendant sécuriser de la connexion Sans fil.

La plupart des scénarios de vulnérabilités ont été signalées pour des clients, où l'attaque typique possible emploiera de faux aps en tant que « homme au milieu » pour intercepter et injecter les trames spécifiques pendant les négociations de sécurité entre le client et le vrai AP (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081). Ce sont le centre de ce document

Un scénario a été décrit attaquant les infrastructures AP qui fournissent les services d'itinérance 802.11r (pi) rapides (CVE-2017-1382), qui est réparé sur le code récemment libéré d'AireOS

Il y a 4 attaques demeurantes contre des protocoles spécifiques de client : STK, TDLS, WNM, qui ne sont pas directement pris en charge par l'infrastructure d'AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088), et sont hors de portée de ce document

En pratique, un attaquant pourrait déchiffrer le trafic pour la session affectée, ou injectez les trames dans un ou deux directions. Il ne fournit pas une manière de décoder le trafic précédemment existant, avant l'attaque, ni il fournira un mécanisme « obtiennent » les kays de cryptage de tous les périphériques dans un SSID donné ou leurs mots de passe PSK ou de 802.1x

Les vulnérabilités sont vraies, et ont un impact important, mais elles ne signifient pas que des réseaux protégés par WPA2 « sont affectés pour toujours », pendant que la question peut être réparée en améliorant les réalisations du client et du côté AP, pour fonctionner correctement dans ces *scénarios de test négatifs* qui ne sont pas actuellement manipulés d'une manière robuste

Ce qui devrait un client faire :

- Pour des vulnérabilités de côté AP : La mise à jour est l'action recommandée si en utilisant le pi si le pi n'est pas nécessaire pour la Voix/services vidéos, évaluent si la caractéristique pi est désactivée jusqu'à ce que la mise à jour au code fixe soit faite. Si utilisant la Voix, évaluez si CCKM est faisable (le côté client doit le prendre en charge), ou mise à jour au code fixe. Si aucun FT/802.11r n'est en service, il n'y a aucun besoin d'améliorer à ce moment
- Pour des vulnérabilités de côté client, améliorez votre visibilité : assurez-vous que la détection d'escroc est activée, couvrant tous les canaux, et une règle de signaler « le SSID géré » pendant que malveillant est créé. Supplémentaire, modifications de configurations de relance d'EAPoL de mise en place qui peuvent limiter ou bloquent entièrement les attaques à exécuter, comme décrit dans ce document

Le bulletin de renseignements principal de référence est chez 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 des versions 8.0 ou plus tard.

Conditions requises

La connaissance du contenu couvert par le bulletin de renseignements de Sécurité mentionné ci-dessus est exigée.

Pour les attaques WPA KRACK, il y a 2 mesures principales que nous pouvons prendre pour protéger les clients qui n'ont pas été corrigés encore.

1. Protection de relance d'EAPoL (EAP au-dessus de RÉSEAU LOCAL)

2. Détection escroc et caractéristiques de personnification du Point d'accès (AP), pour détecter si les outils d'attaque sont utilisés

Protections d'attaque d'EAPoL

Pour vulnerabilities-2017-13077 à 81, il est relativement facile d'empêcher des clients à affecter, utilisant un compteur de relance d'EAPoL réglé à zéro. Cette configuration est disponible dans toutes les versions WLC

Pourquoi ceci fonctionne

Les besoins d'attaque à la relance supplémentaire d'EAPoL du minimum un générée par l'authentificateur pendant la prise de contact de 4 manières, ou pendant la rotation de clé d'émission. Si nous bloquons la génération des relances, l'attaque ne peut pas être appliquée contre la clé passagère du Pairwise Transient Key (PTK) /Groupwise (GTK).

Incidence possible

1. Clients qui sont lents ou peuvent relâcher le traitement initial d'EAPoL M1 (c.-à-d. le premier message de l'échange clé de 4 manières). Ceci est vu à quelques petits clients ou à quelques téléphones, qui peuvent recevoir le M1, et ne pas être prêt au traiter après la phase d'authentification de dot1x, ou faites-le trop lent pour rencontrer un temporisateur court de retransmission

2. Scénarios avec le mauvais environnement rf, ou connexions WAN entre AP et WLC, qui peuvent entraîner une perte de paquets à un certain point sur la transmission vers le client.

Dans les deux scénarios, les résultats seraient qu'une panne d'échange d'EAPoL peut être signalée, et le client sera désauthentifié, elle devra redémarrer l'association et les procédures d'authentification.

Pour diminuer la probabilité d'encourir dans cette question, un plus long délai d'attente devrait être utilisé (1000 millisecondes), pour accorder plus d'heure pour que des clients lents répondent. Le par défaut est 1000msec, mais pourrait avoir été changé à une valeur inférieure manuellement ainsi il doit être vérifié.

Configuration

Il y a deux mécanismes disponibles pour configurer cette modification.

- Global, disponible dans des toutes les releases
- Par WLAN, fourni par 7.6 au plus tard

L'option globale est plus simple, et peut être faite dans des toutes les releases, l'incidence est à travers tous les WLAN dans le WLC.

Par WLAN le paramètre de configuration permet à un contrôle plus granulaire, avec la possibilité pour limiter que le SSID obtient affecté, ainsi les modifications pourraient être appliquées par types de périphérique, etc., si elles sont groupées sur les wlans spécifiques. C'est fourni par la version 7.6

Par exemple, il pourrait être appliqué à un 802.1x générique WLAN, mais pas dans une particularité WLAN de Voix, où il peut avoir une plus grande incidence

Configuration globale #1 :

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

(Option CLI seulement)

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
```

#2 par config WLAN

ID X=WLAN

```
config wlan security eap-params enable X

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

Comment identifier si un client est dû supprimé aux retransmissions zéro

Le client serait dû supprimé aux relances maximum d'EAPoL atteint, et désauthentifié. Le compte de retransmettre est 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 du client PMK/GTK, doivent « présenter » un faux AP avec le même SSID que l'infrastructure AP, mais fonctionnement sur un différent canal. Ceci peut être facilement détecté et l'administrateur réseau peut prendre des mesures physiques basées sur lui, car c'est une activité visible.

Il y a 2 manières proposées jusqu'ici pour faire les attaques d'EAPoL :

- Truquant l'infrastructure AP, en d'autres termes, agissant en tant qu'escroc AP, utilisant le même MAC address, de vrai AP, mais sur un différent canal. Facile à faire pour l'attaquant mais visible
- Injectant des trames dans une connexion valide, forçant le client pour réagir. C'est beaucoup moins visible, mais décelable dans certaines conditions, il peut avoir besoin de synchronisation très

soigneuse pour être réussie

La combinaison des caractéristiques de personnification AP et de la détection escroc peut la détecter si un « faux AP » est placé dans le réseau.

Configuration

- Validez que la détection d'escroc est activée sur les Points d'accès. Ceci est activé par défaut, mais pourrait avoir été désactivé manuellement par l'admin, ainsi il doit être vérifié.
- Créez la règle de signaler des escrocs utilisant « le SSID géré » comme malveillant :
- Assurez-vous que la surveillance de canal est placée à « tous les canaux » pour les deux réseaux 802.11a/b. L'attaque de base est conçue presque pour être de point de vue rf, le client, sur un différent canal de ce qui est utilisé sur l'infrastructure aps. C'est pourquoi il est important de s'assurer que tous les canaux possibles sont balayés :

Personnification AP

Sur la configuration par défaut, l'infrastructure peut la détecter si l'outil d'attaque utilise une de nos adresses de MAC AP. Ceci est signalé comme déroutement SNMP et serait indication que l'attaque a lieu.

```
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 consultatif de Sécurité

Gestion escroc dans un réseau sans fil unifié utilisant v7.4 - Cisco

Pratiques recommandées Sans fil de configuration de contrôleur LAN de Cisco - Cisco

Détection escroc sous des réseaux sans fil unifié - Cisco