Draadloze KRACK-clientzijwerk aan de kant en detectie

Inhoud

[Inleiding](#)
[Gebruikte componenten](#)
[Vereisten](#)
[EAPoL-aanvallen](#)
[Waarom dit werkt](#)
[Mogelijke impact](#)
[Configuratie](#)
[Hoe te identificeren of een client is verwijderd door nul terugzendingen](#)
[Ruggendetectie](#)
[Configuratie](#)
[AP-imitatie](#)
[Referenties](#)

Inleiding

Op 16 oktober is een reeks kwetsbaarheden die algemeen bekend zijn als KRACK en die verschillende protocollen beïnvloeden die in WiFi-netwerken worden gebruikt, openbaar gemaakt. Ze hebben invloed op beveiligingsprotocollen die gebruikt worden op de WAP/WAP2-netwerken. Dit kan de privacy of integriteit van de gegevens in gevaar brengen wanneer ze verspreid worden via een draadloze verbinding.

Het praktische effectniveau varieert aanzienlijk per scenario, plus niet alle cliëntenzijimplementaties worden op dezelfde wijze beïnvloed.
De aanvallen maken gebruik van verschillende slimme scenario's van "negatieve tests", waarbij de transities van de toestand niet correct gedefinieerd zijn op de draadloze standaarden, en in de meeste gevallen niet goed behandeld worden door het betreffende apparaat. Het is niet tegen de crypto algoritmen die worden gebruikt om WAP2 te beschermen, maar over hoe de authenticatie en protocol onderhandelingen tijdens het verzekeren van de draadloze verbinding worden gedaan.

De meeste kwetsbaarheidsscenario's zijn gemeld voor klanten, waar de mogelijke typische aanval nepps als "man in het midden" zal gebruiken om specifieke frames te onderscheppen en te injecteren tijdens de veiligheidsonderhandelingen tussen de klant en de echte AP (CVE-2017-13077, CVE-2017-13078, CVE-201 7-13079, CVE-2017-13080, CVE-2017-13081). Dit is de focus van dit document

Er is een scenario beschreven dat gericht is op de AP-infrastructuur die 802.11r (FT) snelle roamingdiensten (CVE-2017-1382) biedt en die is vastgesteld op de onlangs vrijgegeven AireOS-code

Er zijn nog 4 aanvallen op clientspecifieke protocollen: STK, TDLS, WNM, die niet rechtstreeks worden ondersteund door de AireOS-infrastructuur (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13 88) en vallen buiten het toepassingsgebied van dit document

In praktische termen zou een aanvaller verkeer voor de getroffen sessie kunnen decrypteren of frames in een of twee richtingen kunnen injecteren. Het biedt geen manier om eerder bestaand verkeer, voorafgaand aan de aanval, te decoderen noch het zal een mechanisme voorzien om de encryptie kays van alle apparaten in een bepaalde SSID of hun PSK of 802.1x wachtwoorden te "verkrijgen"

De kwetsbaarheden zijn reëel en hebben een significante impact, maar ze betekenen niet dat netwerken die beveiligd zijn met WAP2 "altijd beïnvloed" zijn, omdat de kwestie kan worden vastgesteld door de implementaties aan zowel client- als AP-zijde te verbeteren, om goed te werken in die *negatieve testscenario's* die momenteel niet robuust worden afgehandeld

Wat moet een klant doen:

- Voor AP-zijkwetsbaarheden: Een upgrade is de aanbevolen actie als FT gebruikt wordt. Als FT niet nodig is voor spraak/video-services, dient u te evalueren of FT-optie uitgeschakeld is totdat de upgrade naar vaste code is uitgevoerd. Als u spraak gebruikt, evalueer dan of CCKM haalbaar is (clientkant moet ondersteunen), of upgrade naar vaste code. Als er geen FT/802.11r in gebruik is, hoeft u momenteel geen upgrade uit te voeren
- Voor kwetsbaarheden aan de kant van de cliënt, verbeter uw zicht: Zorg ervoor dat detectie van abnormaliteiten is ingeschakeld, voor alle kanalen en voor een regel om "beheerde SSID" te melden wanneer kwaadaardig wordt gemaakt. Daarnaast voert u alle mogelijke wijzigingen in de EAPoL-configuraties in die de uit te voeren aanvallen kunnen beperken of geheel blokkeren, zoals in dit document wordt beschreven

Het referentieresearch is te vinden op https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. O

Gebruikte componenten

Dit document is gericht op draadloze controllers die versies 8.0 of hoger uitvoeren.

Vereisten

Kennis van de inhoud van het hierboven genoemde veiligheidsadvies is vereist.

Voor de aanvallen van de KRACK, zijn er 2 belangrijkste acties die we kunnen ondernemen om de cliënten te beschermen die nog niet zijn gepatcheerd.

1. EAPoL (EAP over LAN)-herprobeerbescherming

2. Standaard detectie- en access point (AP)-imitatie-functies, om te detecteren of de aanvalsgereedschappen worden gebruikt

EAPoL-aanvallen

Voor de kwetsbaarheden-2017-13077-81 is het betrekkelijk eenvoudig om te voorkomen dat cliënten worden getroffen, door gebruik te maken van een MAPoL reposte tegen nul. Deze configuratie is beschikbaar in alle WLC-versies

Waarom dit werkt

De aanval moet minstens één extra EAPoL opnieuw proberen die door de authenticator gegenereerd wordt tijdens de handdruk van 4 richtingen, of tijdens de omwenteling van de uitzending sleutel. Als we de generatie van herhalingen blokkeren, kan de aanval niet worden uitgevoerd tegen Pairwise Transient Key (PTK)/Groepswise Transient Key (GTK).

Mogelijke impact

1. Clients die traag zijn of de eerste verwerking van EAPoL M1 kunnen verminderen (d.w.z. het eerste bericht van de uitwisseling van 4 richtingen). Dit wordt gezien bij sommige kleine klanten of sommige telefoons, die de M1 kunnen ontvangen, en niet klaar zijn om het te verwerken na de dot1x authenticatiefase, of het te langzaam doen om aan een korte heruitzending timer te voldoen

2. Scenario's met een slechte RF-omgeving of WAN-verbindingen tussen AP en WLC, die op een bepaald moment een pakketdaling kunnen veroorzaken bij de transmissie naar de client.

In beide scenario's zou het gevolg zijn dat een EMAPoL-valutacalluffect kan worden gerapporteerd en dat de cliënt zal worden gedeconstrueerd, zal hij de associatie- en authenticatieprocessen opnieuw moeten starten.

Om de kans op het aangaan van deze kwestie te verkleinen, moet een langere termijn worden gebruikt (1000 msec), zodat langzame klanten meer tijd hebben om te reageren. De standaardinstelling is 1000msec, maar had handmatig kunnen worden gewijzigd in een lagere waarde zodat dit moet worden geverifieerd.

Configuratie

Er zijn twee mechanismen beschikbaar om deze verandering te configureren.

- Wereldwijd, beschikbaar in alle releases
- Per WLAN, beschikbaar via 7.6 naar nieuwste

De mondiale optie is eenvoudiger en kan in alle releases worden uitgevoerd, is de impact bij alle WLAN's in de WLC.

Per WLAN-configuratie staat een meer granulaire controle toe, met de mogelijkheid om te beperken welke SSID wordt beïnvloed, zodat de wijzigingen per apparaat kunnen worden toegepast, enz., als zij op specifieke bedradingen worden gegroepeerd. Dit is beschikbaar onder versie 7.6

Hij kan bijvoorbeeld worden toegepast op een generiek 802.1x WLAN, maar niet op een spraakspecifieke WLAN's, waar deze een grotere impact hebben

#1 Wereldwijde configuratie:

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

(alleen CLI-optie)

De waarde kan worden gevalideerd met:

```
(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 per WLAN-configuratie

X=WLAN-id

```
config wlan security eap-params enable X

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

Hoe te identificeren of een client is verwijderd door nul terugzendingen

De client wordt verwijderd omdat MAPoL opnieuw wordt uitgevoerd en gedeauthenticeerd. Het aantal overboekingen is 1, aangezien het eerste frame wordt geteld

```
 *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)
```

Ruggendetectie

Verscheidene van de aanvalstechnieken voor de kwetsbaarheden tegen de client-PMK/GTK-encryptie, moeten een nep-AP "presenteren" met dezelfde SSID als de infrastructuur AP, maar opereren op een ander kanaal. Dit kan gemakkelijk worden gedetecteerd en de netwerkbeheerder kan fysieke acties op basis daarvan ondernemen, aangezien het een zichtbare activiteit is.

Tot nu toe zijn er twee manieren voorgesteld om de EAPoL-aanvallen te doen:

- Een gebrek aan AP van de infrastructuur, met andere woorden, handelend als schurken AP, gebruikmakend van hetzelfde hoofdadres, van een echte AP, maar op een ander kanaal. Eenvoudig te doen voor de aanvaller maar zichtbaar
- Het injecteren van frames in een geldige verbinding, dwingt de client om te reageren. Dit is een stuk minder zichtbaar, maar onder sommige omstandigheden detecteerbaar, kan het een zeer zorgvuldige timing vereisen om succes te hebben

De combinatie van AP imitatie eigenschappen en schurkendetectie kan ontdekken als een "nep-ap" in het netwerk wordt geplaatst.

Configuratie

- Bevestig dat schurkendetectie is ingeschakeld op de toegangspunten. Dit wordt standaard ingeschakeld maar kan handmatig door de beheerder worden uitgeschakeld. Dit moet worden geverifieerd.
- Regel maken om werkbalken te markeren met "beheerde SSID's" als kwaadaardig:
- Zorg ervoor dat de kanaalcontrole voor beide 802.11a/b-netwerken op "alle kanalen" is ingesteld. De basisaanval is ontworpen om in de buurt te zijn van RF perspectief, de cliënt, op een ander kanaal dan wat op de infrastructuur APs wordt gebruikt. Daarom is het belangrijk ervoor te zorgen dat alle mogelijke kanalen gescand worden:

AP-imitatie

Bij de standaardconfiguratie kan de infrastructuur detecteren als het aanvalsgereedschap een van onze AP-hoofdadressen gebruikt. Dit wordt gemeld als een SNMP-val en zou betekenen dat de aanslag plaatsvindt.

```
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
```

Referenties

Veiligheidsadvisering

Gespreksbeheer in een Unified Wireless Network op basis van v7.4 - Cisco

Configuratie van Cisco draadloze LAN-controllers - beste praktijken voor Cisco

Soortdetectie onder Unified draadloze netwerken - Cisco