無線KRACK攻擊客戶端的變通和檢測

目錄

[簡介](#)
[採用元件](#)
[需求](#)
[EAPoL攻擊保護](#)
[為什麼這樣有效](#)
[可能的影響](#)
[組態](#)
[如何確定客戶端是否由於零重傳而被刪除](#)
[欺詐檢測](#)
[組態](#)
[AP模擬](#)
[參考資料](#)

簡介

10月16日，一組被廣泛稱為KRACK的漏洞被公之於眾，這些漏洞影響WiFi網路中使用的不同協定。它們影響在WPA/WPA2網路上使用的安全協定，當通過無線連線傳輸資料時，這些協定可能會損害資料隱私或完整性。

實際影響水準對每種方案都有很大差異，而且並非所有客戶端實施都會受到相同的影響。
這些攻擊使用不同的「負面測試」的巧妙方案，即在無線標準上未正確定義的狀態轉換被嘗試，在大多數情況下，受影響裝置未正確處理。這不是針對用於保護WPA2的加密演算法，而是針對在無線連線安全期間如何進行身份驗證和協定協商。

大多數漏洞場景都針對客戶端進行了報告，其中可能的典型攻擊會使用假冒接入點作為「中間人」，在客戶端與實際AP的安全協商過程中攔截並注入特定幀(CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081)。 以下是本文的重點

描述了一個攻擊提供802.11r(FT)快速漫遊服務的AP基礎設施(CVE-2017-1382)的場景，該場景已在最近發佈的AireOS代碼上修復

針對客戶端特定協定還剩下4次攻擊：STK、TDLS和WNM，它們不受AireOS基礎架構直接支援(CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088)，並且不屬於本文檔範圍

在實際操作中，攻擊者可以解密受影響會話的流量，或者在一個或兩個方向注入幀。它不提供在攻擊前解碼先前現有流量的方法，也不提供「獲取」給定SSID中所有裝置的加密金鑰或其PSK或802.1x密碼的機制

這些漏洞是真實存在的，而且影響顯著，但是它們並不表示WPA2保護的網路會「永遠受影響」，因為可以通過改進客戶端和AP端的實施來修復此問題，以便在當前未以可靠方式處理的負面測試場景中正常運*作*

客戶應該怎麼做：

- 對於AP端漏洞：如果使用FT，則升級是推薦的操作。如果語音/影片服務不需要FT，請評估是否應在完成升級到固定代碼之前禁用FT功能。如果使用語音，請評估CCKM是否可行（客戶端需要支援），或者升級到固定代碼。如果未使用FT/802.11r，此時無需升級
- 針對客戶端漏洞，提高可視性：確保已啟用涵蓋所有通道的欺詐檢測，並建立將「託管SSID」報告為惡意的規則。此外，實施可限制或完全阻止要執行的攻擊的EAPoL重試配置更改，如本文檔所述

主要參考諮詢位於https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa。T

採用元件

本檔案將重點介紹執行8.0或更新版本的無線控制器。

需求

需要瞭解上述安全建議涵蓋的內容。

對於WPA KRACK攻擊，我們可以採取兩個主要操作來保護尚未修補的客戶端。

1. EAPoL(EAP over LAN)重試保護

2.欺詐檢測和接入點(AP)模擬功能，檢測是否正在使用攻擊工具

EAPoL攻擊保護

對於vulnerabilities-2017-13077 to 81，使用EAPoL重試計數器設定為零相對容易防止客戶端受到影響。 此組態在所有WLC版本中可用

為什麼這樣有效

該攻擊至少需要身份驗證器在4次握手期間或廣播金鑰旋轉期間生成一次額外的EAPoL重試。如果阻止重試的生成，則無法對Pairwise Transient Key(PTK)/Groupwise Transient Key(GTK)應用攻擊。

可能的影響

1.處理速度慢或可能丟棄EAPoL M1初始處理的客戶端（即4路金鑰交換的第一條消息）。 這在一些小型客戶端或某些電話上出現，這些電話可能接收M1，但在dot1x身份驗證階段後尚未準備好處理它，或者執行速度太慢而無法滿足短重傳計時器

2. RF環境不佳或AP和WLC之間的WAN連線不佳的情況，可能導致資料包在向客戶端傳輸時的某個點丟失。

在這兩種情況下，結果都是EAPoL交換失敗可能被報告，並且客戶端將被取消身份驗證，這將必須重新啟動關聯和身份驗證過程。

為了降低發生此問題的可能性，應該使用更長的逾時（1000毫秒），以便更慢的客戶端有更多時間響應。預設值為1000毫秒，但可能手動更改為較低的值，以便進行驗證。

組態

有兩種機制可用於配置此更改。

- 全域性，在所有版本中可用
- 每個WLAN，從7.6到最新版本

全域選項更簡單，且可以在所有版本中完成，因此影響將遍及WLC中的所有WLAN。

每個WLAN配置設定允許更精細的控制，並可能限制哪個SSID受到影響，因此如果更改在特定WLAN上分組，則可以按裝置型別等應用更改。7.6版提供

例如，它可以應用於通用802.1x WLAN，但不能應用於語音特定的WLAN，因為在WLAN中可能會產生更大的影響

#1 Global Config:

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

（僅限CLI選項）

可以使用以下工具驗證該值：

```
(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每WLAN配置

X=WLAN ID

```
config wlan security eap-params enable X

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

如何確定客戶端是否由於零重傳而被刪除

由於達到最大EAPoL重試次數，因此將刪除客戶端，並取消身份驗證。重新傳輸計數為1，因為初

始幀已計數

```
 *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)
```

欺詐檢測

針對客戶端PMK/GTK加密的漏洞的幾種攻擊技術需要「呈現」一個虛假AP，該AP的SSID與基礎架構AP相同，但在不同的通道上運行。這可以很容易地檢測到，網路管理員可以基於它採取物理操作，因為這是一個可見的活動。

目前針對EAPoL攻擊提出了兩種方法：

- 偽造基礎設施AP，換句話說，使用相同的MAC地址作為惡意AP，但使用不同的通道。對攻擊者而言易於操作，但可見
- 將幀注入有效的連線，迫使客戶端作出反應。雖然這不太容易看見，但在某些情況下可檢測到，它時點可能需要非常小心的時間，才能成功

AP模擬功能和欺詐檢測結合起來可以檢測網路中是否放置了「假ap」。

組態

- 驗證接入點上是否已啟用欺詐檢測。預設情況下，這是啟用的，但管理員可能已手動禁用，因此要進行驗證。
- 建立使用「託管SSID」將欺詐標籤為惡意的規則：
- 確保將兩個802.11a/b網路的通道監控設定為「所有通道」。從射頻的角度來看，基本攻擊設計為靠近客戶端，位於與基礎設施AP所用通道不同的通道上。這就是確保掃描所有可能通道的原因：

AP模擬

在預設配置中，基礎架構可以檢測攻擊工具是否使用我們的AP MAC地址。此陷阱被報告為SNMP陷阱，表示攻擊正在發生。

```
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
```

參考資料

安全建議通知

使用v7.4的統一無線網路中的欺詐管理 — 思科

思科無線區域網控制器配置最佳實踐 — Cisco

統一無線網路下的欺詐檢測 — Cisco