ワイヤレス KRACK 攻撃クライアント側回避策および検出

目次

概要

10 月 16 日に、広く WiFi ネットワークで使用される異なるプロトコルに影響を与える KRACK として知られている一組の脆弱性は公共になされました。 それらは無線接続に送信されるときデータ 機密性か統合を妥協する可能性がある WPA/WPA2 ネットワークで使用されるセキュリティ プロトコルに影響を与えます。

影響の実用的なレベルはすべてのクライアント側実装と各シナリオで、同じように影響を受けますかなり異なりません。
不正侵入は適切にワイヤレス規格で定義されない状態遷移が試みられる、ほとんどの場合、影響を受けたデバイスによってきちんと処理されなくて使用しところで「ネガティブ テスト」の異なる利発なシナリオを。 認証およびプロトコルネゴシエーションが無線接続の保護の間にどのようにに行われるかない WPA2 を保護することを使用される暗号 アルゴリズムに対してありませんが。

脆弱性シナリオのほとんどはクライアントと実質 AP （ CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081 ）間のセキュリティ ネゴシエーションの間に特定の帯を代行受信し、インジェクトするのに可能性のある典型的な攻撃が「中央の人」として擬似 APS を使用するクライアントのために報告されました。 これらはこの資料のフォーカスです

802.11r （ FT ）ファースト ローミングサービスを（ CVE-2017-1382 ）提供する AP インフラストラクチャを攻撃する 1 シナリオは解説されていました、最近 AireOS リリースされたコードで固定される

クライアント特定のプロトコルに対して 4 つの残りの不正侵入があります: STK は、TDLS、この資料の範囲外に AireOS インフラストラクチャ（ CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088 ）によって直接サポートされない、およびあります WNM

実際問題としては、攻撃者は影響を受けたセッションのためのトラフィックを復号化する可能性がありますまたは 1-2 方向の帯をインジェクトして下さい。 それは攻撃前に以前に トラフィックを、存在 することをデコードする方法を提供しませんメカニズムを「得ます」ある特定の SSID または PSK または 802.1X パスワードのすべてのデバイスの暗号化 kays を提供します

脆弱性は実質でが、重大な影響があります、問題がクライアントおよび AP 側両方の実装の改善によって解決することができると同時に WPA2 保護されたネットワークが強い方法で現在処理されないそれらの*否定的なテストシナリオ*できちんとはたらくために「永久に」影響を受けることを意味しません

顧客必要がある何がする:

- AP 側脆弱性に関しては: アップグレードは修正されたコードへのアップグレードが実行されるまで FT 機能が無効である場合 FT が音声/ビデオ サービスのために必要でなければフィートを使用している、評価する場合推奨 処置です。 音声を使用している場合、CCKM が実行可能 (クライアント側はサポートする必要があります) 、またはアップグレード 修正されたコードに評価して下さい。 FT/802.11r が使用中ではない場合、現時点でアップグレードする必要がありません
- クライアント側脆弱性に関しては、表示を改善して下さい: 悪意のあると同時にすべてのチャネルをカバーする悪党検出が有効に なる「管理された SSID」を報告するルール作成されますようにすれば。 さらに、制限できたりまたは完全に実行されたべき不正侵入をブロックするこの資料に記述されているように実装する EAPoL 再試行設定変更

主要な参照アドバイザリは https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa にあります。 T

使用するコンポーネント

この資料はリリース 8.0 またはそれ以降を実行しているワイヤレス コントローラに焦点を合わせます。

要件

上記される Security Advisory によってカバーされるコンテンツのナレッジは必要となります。

WPA KRACK 不正侵入に関しては、まだ修正されていないクライアントを保護するためにとることができる 2 つの主要な処置があります。

1. EAPoL （ EAP over LAN ）再試行保護

2. 攻撃ツールが使用される場合不正な検出および Access Point （ AP ）偽装機能、検出するため

EAPoL 攻撃保護

81 への vulnerabilities-2017-13077 に関しては、ゼロに設定される EAPoL リトライ カウンタを使用して、影響を受けるべきクライアントを防ぐことは比較的容易です。 この設定はすべての WLC バージョンで利用できます

これがなぜはたらくか

EAPoL 追加再試行少くとも 1 の攻撃必要 4 つの方法ハンドシェイク、またはブロードキャスト キー ローテーションの間にオーセンティケータによって生成される。 再試行の生成をブロックする場合、攻撃はトランジェント キー（PTK）/Groupwise トランジェント キー（GTK）に対して一対に適用します。

可能性のある影響

1. 遅かったりまたは EAPoL M1（すなわち 4 つの方法鍵交換の最初のメッセージ）の最初の処理を廃棄するかもしれないクライアント。 これはおよび dot1x 認証フェーズ以降にそれを処理して準備ができていないために見られます M1 を受け取るかもしれないまたは遅いそれを短い再送信 タイマーに会うには余りにもして下さいいくつかの電話か何人かの小さいクライアントで

2. 悪い RF 環境のシナリオ、かクライアントの方の伝達のパケット破棄をある時点で引き起こすかもしれない WLC、と AP 間の WAN 接続。

両方のシナリオで、結果は EAPoL 交換失敗が報告されることがあるクライアントは deauthenticated ことであり、アソシエーションおよび認証プロセスを再起動しなければなりません。

負う確率をこの問題に減少させるために、応答するより長いタイムアウトが（1000 ミリ秒）、遅いクライアントのより多くの時間を認めるのに使用する必要があります。 デフォルトは 1000msec ですが、より低い値に手動で変更されたかもしれません従ってそれは確認されるべきです。

設定

利用可能 な 2 つのメカニズムがこの変更を設定するためにあります。

- グローバル、すべてのリリースで利用可能
- 7.6 から最も遅くに利用可能 な WLAN ごと

グローバル オプションは WLC のすべての WLAN を渡ってより簡単で、すべてのリリースで影響ありますすることができます。

WLAN コンフィギュレーションの設定ごとに特定の wlans でグループ化される場合影響を与えられた SSID gets が従って変更デバイスの種類、等ごとに適用する可能性がある可能性の粒状制御が、制限するようにします。 これはバージョン 7.6 から利用可能です

たとえば、それは一般的 な 802.1X WLAN に、ないより大きい影響があるかもしれない音声仕様 WLAN に適用できます

#1 グローバル設定:

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

（CLI オプションだけ）

値は下記のもので検証することができます:

```
(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
```

WLAN 構成ごとの #2

X=WLAN ID

```
config wlan security eap-params enable X

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

クライアントがゼロ再送信が削除された原因である場合識別する方法

達されたおよび deauthenticated クライアントは EAPoL 最大再試行が削除された原因です。 再送信数は最初 の フレームが数えられるので、1 です

```
 *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)
```

不正検出

クライアント PMK/GTK 暗号化に対する脆弱性のための攻撃手法の複数は、同じ SSID の擬似 AP を「示す別のチャネルのインフラストラクチャ AP、操作と」必要があります。 これは容易に検出する、ネットワーク管理者はそれが目に見えるアクティビティであるのでそれに基づいて物理的 な処置をとることができます。

EAPoL 不正侵入をするためにこれまでのところ提案される 2 つの方法があります:

- すなわち、インフラストラクチャ AP を、偽造し、実質 AP の、しかし別のチャネルの同じ MAC アドレスを使用して、不正な AP として機能します。 攻撃者のためにすること容易しかし目に見える
- 帯を反応させますクライアントを有効な接続にインジェクトします。 これはたくさんより少なく目に見えます、しかし探索可能ある条件で、非常に注意深いタイミングが正常であることを必要とする場

合もあります
AP 偽装機能および不正な検出の組み合せは「擬似 ap」がネットワークに置かれる場合検出することができます。

設定

- 悪党検出がアクセス ポイントで有効に なること検証して下さい。 これはデフォルトで有効に なりますが、admin によって手動でディセーブルにされたかもしれません従ってそれは確認されるべきです。
- 悪意のあるように「管理された SSID」を使用している悪党にフラグを付けるルールを作成して下さい:
- チャネル モニタリングが両方の 802.11a/b ネットワークのための「すべてのチャネル」に設定 されるようにして下さい。 基礎攻撃は RF 観点から使用されるものがからのインフラストラクチャ AP で、別のチャネルのクライアント近くあるように、設計されています。 こういうわけですべての可能性のあるチャネルがスキャンされるようにすることは重要です:

AP 偽装

デフォルト 設定で、インフラストラクチャは攻撃ツールが AP MAC アドレスの 1 つを使用している場合検出することができます。 これは SNMPトラップとして攻撃が起こっているという報告され、しるしです。

```
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
```

参考資料

Security Advisory 表記

v7.4 を使用して Unified Wireless Network の不正な管理- Cisco

Ciscoワイヤレス LAN コントローラ設定 最良 の 方法- Cisco

Unified Wireless Network の下の不正な検出- Cisco