无线KRACK攻击客户端应急方案和检测

目录

简介

在十月16，一般叫作KRACK的一套漏洞影响用于WiFi网络的不同的协议被公开了。他们影响在WPA/WPA2网络使用的安全协议，可能减弱数据保密性或完整性，当在无线连接时传送。

影响显著变化的实用的级别在每个方案，加上不是所有的客户端实施相似地受影响。
攻击使用“负测试”在无线标准不适当地定义的状态转换尝试的地方和在大多数情况下不同的聪明的方案，没适当地处理由受影响的设备。它没有用于的crypto算法保护WPA2，然而关于怎样验证和协议协商完成在期间保护无线连接。

大多漏洞方案为客户端报告，可能的典型的攻击在中部将使用假Aps作为“人”在客户端和实时AP (CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080， CVE-2017-13081)之间的安全协商中拦截和注入特定帧。这些是本文焦点

描述攻击提供802.11r的AP基础设施的一个方案(FT)快速地漫游服务(CVE-2017-1382)，在最近发布的AireOS代码修复

有4剩余的攻击客户端特定协议：STK， TDLS， WNM， AireOS基础设施不直接地支持(CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088)，在本文的范围之外，和是

用实际的话说，攻击者可能解密受影响的会话的流量，或者请注入在一两个方向的帧。它不提供一个方式在攻击之前解码以前现有流量，亦不将提供一机制“获取”所有设备加密kays在一给的SSID或他们的PSK或者802.1x密码的

漏洞实时，并且有重大影响，但是他们不意味着WPA2受保护的网络“在当前没有被处理用一个稳健方式的那些*负测试方案*受影响得永久”，当问题可以通过改善在客户端的实施修复，并且AP支持，适当地运作

什么应该客户执行：

- AP侧漏洞：升级是推荐的操作，如果使用英尺，如果FT为语音/视频服务不是需要的，评估，如果FT功能应该禁用，直到对固定的代码的升级完成。如果曾经语音，请评估，如果CCKM可行(客户端需要支持)，或者升级对固定的代码。如果FT/802.11r不是在使用中的，没有需要此时升级
- 对于客户端漏洞，请改进您的可见性：保证歹徒检测启用，包括所有信道和规则报告“管理的SSID”，当有恶意创建。另外，请实现EAPoL重试次数能限制或完全地拦截将执行的攻击的配置更改，正如本文所描述

主要参考建议在https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa。T

使用的组件

本文着重运行版本8.0或以上的无线控制器。

要求

安全建议包括的内容的知识以上提到要求。

对于WPA KRACK攻击，有我们能采取保护客户端未被修补的2次主要行动。

1. EAPoL (EAP over LAN)重试次数保护

2. 恶意检测和接入点(AP)模拟功能，检测，如果使用攻击工具

EAPoL攻击保护

对于vulnerabilities-2017-13077到81，防止使用EAPoL重试次数计数器将受影响的，客户端调整到零是相对容易的。 此配置有所有WLC版本

这为什么工作

在验证器生成的最低一另外的EAPoL重试次数的攻击需要在4种方式握手期间，或者在广播密钥交替时。如果我们阻塞重试次数的生成，攻击不可能成对地应用临时密钥(PTK) /Groupwise临时密钥(GTK)。

潜在影响

1. 即慢或可能下降最初处理EAPoL M1的客户端(第一条消息4种方式密钥交换)。这在一些小客户端或一些电话被看到，可能接收M1和不准备在dot1x认证阶段之后处理它，或者请执行它太慢以至于不能满足一个短的重新传输计时器

2. 与坏RF环境的方案或者AP和WLC之间的广域网连接，可能导致一丢包在往客户端的发射。

在两种情况下，结果是EAPoL交换失败可能报告，并且客户端deauthenticated，将必须重新启动关联和认证过程。

要减小可能性导致到此问题，应该用于一更加长的超时(1000毫秒)，允许慢客户端的更多时刻响应。默认是1000msec，但是可能手工更改到较低值，因此将验证。

配置

有可用两的机制配置此更改。

- 全局，在所有版本的联机
- 每WLAN，从7.6的可得到到新

全局选项更加简单，并且可以执行在所有版本，影响是在WLC的所有WLAN间。

每个WLAN配置设置允许一更加粒状的控制，以被影响的SSID获得，因此更改可能每设备类型等等应用的可能性限制，如果他们在特定WLAN分组。这从版本7.6是可得到

例如，它可能应用到一通用的802.1x WLAN，但是不到语音特定WLAN，可能有一更加大的影响

#1全局配置：

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

(CLI唯一选择)

值可以验证与：

```
(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
```

每WLAN设置的#2

X=WLAN ID

```
config wlan security eap-params enable X

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

如何识别，如果客户端删除的归结于零的重新传输

客户端删除的归结于最大EAPoL重试次数被到达和deauthenticated。因为初始帧计算，重新传输计数是1

```
 *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)
```

入侵检测

数漏洞的攻击技术客户端PMK/GTK加密，需要“提交”与SSID的伪造品AP和基础设施AP，但是操作在一个不同的信道一样。这可以容易地检测，并且网络管理员能采取根据它的物理行动，因为它是一个可视活动。

到目前为止有报价的2种方式执行EAPoL攻击：

- 伪造基础设施AP，换句话说，作为非法AP，使用同样MAC地址，实时AP，但是在一个不同的信道。容易为攻击者执行，但是可视
- 注入帧有效连接，迫使客户端起反应。这很多较不可视，但是可发现在某些条件下，可能需要非常仔细定时是成功的

如果“伪造品ap”在网络，安置AP模拟功能和恶意检测的组合能检测。

配置

- 验证歹徒检测在接入点启用。默认情况下这启用，但是可能由admin手工禁用，因此将验证。
- 创建规则标记使用“管理的Ssid的”歹徒如有恶意：
- 保证信道监听设置为“所有信道”两802.11a/b网络的。基本攻击设计近从RF方面，客户端，从什么的一个不同的信道的在基础设施AP使用。这就是为什么请注意所有可能的信道被扫描：

AP模拟

在默认配置，如果攻击工具使用我们的一AP MAC地址，基础设施能检测。这报告作为SNMP陷阱，并且是暗示攻击发生。

```
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
```

参考

安全建议公告

在一统一无线网络的恶意管理使用v7.4 -思科

Cisco无线LAN控制器配置最佳实践-思科

在Unified无线网络下的恶意检测-思科