无线KRACK攻击客户端解决方法和检测

目录

简介

10月16日，WiFi网络中使用的不同协议被公之于众的KRACK漏洞集被公之于众。它们会影响WPA/WPA2网络上使用的安全协议，当通过无线连接传输数据时，这些协议可能会损害数据隐私或完整性。

每种场景的实际影响级别会有很大不同，而且并非所有客户端实施都以相同的方式受到影响。攻击使用不同的“负面测试”聪明场景，在这些场景中，未在无线标准上正确定义状态转换，在大多数情况下，受影响的设备未正确处理状态转换。它不针对用于保护WPA2的加密算法，而是针对在保护无线连接期间如何进行身份验证和协议协商。

大多数漏洞场景都针对客户端报告，在客户端与实际AP(CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-201)安全协商期间，可能的典型攻击会使用假Ap作为“中间人”拦截并注入特定帧7-13080、CVE-2017-13081)。 以下是本文档的重点

描述了一种攻击提供802.11r(FT)快速漫游服务(CVE-2017-1382)的AP基础设施的场景，该场景在最近发布的AireOS代码上修复

针对客户端特定协议的攻击还有4种：STK、TDLS、WNM，AireOS基础设施(CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088)不直接支持，不在本文档的范围内

实际上，攻击者可以解密受影响会话的流量，或向一个或两个方向注入帧。它不提供在攻击前解码先前现有流量的方法，也不提供“获取”给定SSID中所有设备的加密密钥或其PSK或802.1x密码的机制

这些漏洞是真实的，并且会产生重大影响，但它们并不意味着WPA2保护的网络会“永远受到影响”，因为通过改进客户端和AP端的实施可以解决此问题，以便在当前未以稳健方式处理的负*面测试情*景中正常工作

客户应该做什么：

- 对于AP端漏洞：如果语音/视频服务不需要FT，则建议使用升级。在完成对固定代码的升级之前，评估是否应禁用FT功能。如果使用语音，请评估CCKM是否可行（客户端需要支持），或升级到固定代码。如果没有FT/802.11r在使用，此时无需升级
- 对于客户端漏洞，请提高您的可视性：确保已启用欺诈检测，覆盖所有信道，并创建将“托管SSID”报告为恶意的规则。此外，实施EAPoL重试配置更改，这些更改可以限制或完全阻止要执行的攻击，如本文档所述

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

使用的组件

本文档重点介绍运行8.0或更高版本的无线控制器。

要求

需要了解上述安全建议涵盖的内容。

对于WPA KRACK攻击，我们可以采取2项主要措施来保护尚未修补的客户端。

1. EAPoL(EAP over LAN)重试保护

2.欺诈检测和接入点(AP)模拟功能，用于检测是否正在使用攻击工具

EAPoL攻击保护

对于漏洞 — 2017-13077到81，使用EAPoL重试计数器设置为零来防止客户端受到影响相对容易。此配置在所有WLC版本中都可用

为什么这样做

攻击至少需要身份验证器在四次握手期间或广播密钥轮替期间生成一次额外的EAPoL重试。如果阻止重试的生成，则无法对成对临时密钥(PTK)/分组临时密钥(GTK)应用攻击。

可能的影响

1.客户端速度慢或可能丢弃EAPoL M1的初始处理（即4路密钥交换的第一条消息）。 在某些小型客户端或某些电话上会看到这种情况，这些客户端可能接收M1，但在dot1x身份验证阶段后未准备好处理它，或者速度太慢，无法满足短的重新传输计时器

2. RF环境不良或AP和WLC之间WAN连接不良的情况，可能导致数据包在传输到客户端的某个点丢弃。

在这两种情况下，结果都是可能报告EAPoL交换故障，并且客户端将取消身份验证，它必须重新启动关联和身份验证过程。

要降低发生此问题的可能性，应使用更长的超时时间（1000毫秒），以留出更多时间让慢速客户端做出响应。默认值为1000毫秒，但可能已手动更改为较低值，以便进行验证。

配置

有两种机制可用于配置此更改。

- 全局，适用于所有版本
- 每个WLAN，从7.6到最新

全局选项更简单，可在所有版本中执行，其影响在WLC中的所有WLAN中。

根据WLAN配置设置，可以进行更精细的控制，并限制受影响的SSID，因此，如果更改按特定WLAN分组，则可以按设备类型等应用更改。可从版本7.6获得

例如，它可以应用于通用802.1x WLAN，但不能应用于语音特定WLAN，在语音特定WLAN中，它可能会产生较大影响

#1全局配置：

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

（仅CLI选项）

值可通过以下方式验证：

```
(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每个WLAN配置

X=WLAN ID

```
config wlan security eap-params enable X

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

如何识别客户端是否因零重新传输而被删除

由于达到最大EAPoL重试次数并取消身份验证，客户端将被删除。重发计数为1，因为初始帧被计

数

```
 *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

针对客户端PMK/GTK加密漏洞的几种攻击技术需要“呈现”与基础设施AP具有相同SSID的假AP，但操作在不同的信道上。这很容易被检测到，网络管理员可以根据它采取物理操作，因为它是可见的活动。

到目前为止，有2种方法被提议用于EAPoL攻击：

- 假装基础设施AP，换句话说，使用相同的MAC地址，在不同的信道上充当恶意AP。对攻击者来说易于操作，但可见
- 将帧注入有效连接，迫使客户端做出反应。这个可见性要低很多，但在某些条件下可以探测到，它可能需要非常谨慎的时间才能成功

AP模拟功能和欺诈检测的组合可以检测网络中是否存在“假AP”。

配置

- 验证接入点上是否启用了欺诈检测。默认情况下，此功能已启用，但管理员可能已手动禁用，因此需要验证。
- 创建规则，将使用“托管SSID”的欺诈标记为恶意：
- 确保将两个802.11a/b网络的信道监控设置为“所有信道”。基本攻击旨在从射频（即客户端）的角度来看，与基础设施AP上使用的攻击处于不同的信道。因此，确保扫描所有可能的信道非常重要：

AP模拟

在默认配置下，基础设施可以检测攻击工具是否使用了我们的AP MAC地址。这被报告为SNMP陷阱，表明攻击正在发生。

```
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

安全建议通知

使用v7.4的统一无线网络中的欺诈管理 — 思科

思科无线局域网控制器配置最佳实践 — 思科

统一无线网络下的欺诈检测 — 思科