WiFi网络WPA2 KRACK漏洞分析报告

阿里聚安全 / 2017-10-19 01:55:51 / 浏览数 3919 安全技术 漏洞分析 顶(0) 踩(0)

作者：阿里安全技术平台团队

0x00 漏洞概述

安全研究员Mathy Vanhoef发现的WPA2协议的KRA（Key Reinstallation Attacks）漏洞，利用WPA2协议标准加密密钥生成机制上的设计缺陷，四次握手协商加密密钥过程中第三个消息报文可被篡改重放，导致在用密钥被重新安装。

WiFi网络通过WPA2 handshake四次握手消息协商用于后续数据通信的加密密钥，其中交互的第三个消息报文被篡改重放，可导致中间人攻击重置重放计数器(replay counter)及随机数值(nonce)，重放给client端，使client安装上不安全的加密密钥。

此漏洞攻击方式被命名为Key reinstallation attacks密钥重装攻击，除了影响已经在用的数据加密密钥，同时也影响PeerKey, group key, Fast BSS切换FT握手等，会导致WiFi通信数据加密通道不安全，存在被嗅探、篡改和重放等风险，攻击者可获取WiFi网络中的数据信息。

几乎所有支持Wi-Fi的设备（Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys等）都面临安全威胁，危害较大。

该漏洞相关影响取决于被攻击的握手过程和数据加密协议，例如AES-CCMP可被重放和解密，TCP流量存在被劫持和注入恶意流量的可能，WPATKIP和GCMP可被重放、篡

相关CVE如下，其中每个CVE代表一种特定场景下的密钥重装攻击。

- CVE-2017-13077: 四次握手过程中重装PTK-TK加密密钥对
- CVE-2017-13078: 四次握手过程中重装GTK
- CVE-2017-13079: 四次握手过程中重装IGTK
- CVE-2017-13080: Group key 握手过程中重装GTK
- CVE-2017-13081: 握手过程中重装IGTK
- CVE-2017-13082: 接收重传的快速BSS切换重关联请求，在处理过程中重安装PTK-TK加密密钥对
- CVE-2017-13084: 在PeerKey握手过程中重安装STK KEY
- CVE-2017-13086: 在DTLS握手过程中重安装TDLS PeerKey
- CVE-2017-13087: 在处理WNM睡眠模式响应帧过程中重安装GTK
- CVE-2017-13088: 在处理WNM睡眠模式响应帧过程中重安装IGTK

漏洞攻击演示视频：

https://www.youtube.com/watch?v=BtdN1SM5Z5o

0x01 WPA2协议介绍

WPA全名为Wi-Fi Protected Access，有WPA和WPA2两个标准, WPA（Wi-Fi Protected Access）加密方式目前有四种认证方式：WPA、WPA-PSK、WPA2、WPA2-PSK，采用的加密算法有两种：AES（Advanced Encryption Standard高级加密算法）和TKIP（Temporal Key Integrity Protocol临时密钥完整性协议）。

由于WEP已被证明为不安全的协议，在802.11i协议完善前，采用WPA为用户提供一个临时性的解决方案。该标准的数据加密采用TKIP协议(Temporary Key Integrity Protocol)，TKIP的两个主要功能是：逐包密钥及消息完整性检查（MIC），与WEP相同的加密算法RC4来实现这一点，虽然TKIP解决了所有已知的WEP问题，但WPA2的A

WPA2是WPA的增强型版本，与WPA相比，WPA2新增了支持AES的加密方式，采用AES加密机制。

0x02 Key reinstallation attacks密钥重装攻击

四次握手协商密钥过程中消息报文见图1EAPOL格式，其中重放计数replay counter字段用于检测重复报文，每次发送一个报文，重放计数加一，nonce字段为加密密钥生成所需要的随机数。

图1 EAPOL帧简化报文格式

以group key为例，首先Client进入PTK-INIT状态，初始化(PMK)，当接收到消息1进入PTK_START状态，client会生成随机数SNonce，计算临时TPTK，发送消息2（带SNonce）到 counter重放计数等有效的条件下，进入PTK-NEGOTIATING协商状态，同时标记TPTK为有效，发送消息4到AP，然后直接进入PTK-DONE状态,使用MLME-SETKEYS安装K

图2 四次握手状态机，KEY用MLME-SETKEYS.request命令字进行安装

当client作为Supplicant加入wifi网络，client与AP认证端Authenticator进行四次握手协商新的加密密钥，见下图3，在接收到四次握手中的第3个消息报文时会安装新生成的

因为报文可能丢失，如果AP未接收到client的响应会重发第三个消息报文，所以client可能重复接收到第3个消息报文多次。每次当client接收到此消息，都会重新安装相同的

攻击者可通过嗅探、重放四次握手过程中的第3个消息报文，强制重置协议加密使用到的nonce值及重放计数，重安装加密密钥，从而攻击协议的加密机制，数据报文可被重

该攻击方法同时可用于攻击已在使用的加密密钥、group key、PeerKey, TDLS及快速BSS切换握手等。

图3 Group Key场景四次握手

0x03 漏洞根因分析及影响

802.11协议标准仅提供描述粗粒度的伪码描述四次握手的状态机，但并未清晰描述特定的握手消息应该在什么时候处理。

密钥重装漏洞滥用了消息3重传的流程，首先在Client和AP之间确定MitM中间人攻击的点，在AP接收到消息4之前不断重传篡改后的消息3，导致Client重新安装已用的加密

实际情况，实施此攻击的时候，并非所有的Wi-Fi客户端client都正确实现了此状态机，Windows和iOS未接收处理消息3的重传，这违背了802.11标准，所以密钥重装漏洞攻
key握手的场景下仍然存在安全漏洞，此外在FT握手情况下仍可能被间接攻击。

对于Android 6.0影响更大，在此攻击的情况下，强制使用了可预测全零的加密密钥。

密钥重装漏洞攻击实际影响如下图4，第一列代表不同类型的Client客户端，第2列表示不同Client类型是否接受消息3，第三列表示如果PTK配置，EAPOL消息明文是否接收

特别需要注意的，研究者当前并没有破解Wi-Fi网络的密码，也并没有通过四次握手协商过程的攻击破解新生成的加密密钥。

图4不同Clients的实际漏洞效果

0x04 漏洞影响范围

此漏洞存在于协议标准设计缺陷，所有支持WPA2的客户端都受到影响。

攻击主要面向WPA2客户端设备。

0x05 漏洞安全加固建议

1、 漏洞攻击需要实施MitM中间人攻击，条件许可建议合理部署无线入侵防御系统或者VPN加密，及时监测恶意钓鱼WiFi，禁止私搭AP等；

2、 及时升级此漏洞的安全补丁（有补丁的情况），更新WPA2客户端到最新版本；

3、 仅连接可信wifi，公共场合尽量使用蜂窝移动网络，wifi连接不用的情况下建议禁用，攻击面最小化。

注：

Linux的hostapd和wpa_supplicant补丁已公布，详见 <https://w1.fi/security/2017-1/>。

微软在Windows 10操作系统中发布补丁KB4041676。

苹果在最新的beta版本iOS等中修复了无线网络安全漏洞。

参考文档:

[1] <https://papers.mathyvanhoef.com/ccs2017.pdf>

[2]<https://techcrunch.com/2017/10/16/wpa2-shown-to-be-vulnerable-to-key-reinstallation-attacks/>

上一篇：如何利用威胁情报追踪攻击者 下一篇：爱奇艺业务安全风控体系的建设实践

1. 1 条回复


wooy0ung6 2017-10-19 07:18:15

热点已过

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板