预警编号：YJ-2017025

恒安嘉新

关于 WPA2 无线网络存在密钥重装漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 10 月 17 日

1 漏洞描述

近期 ,互联网爆出多个 WPA2 无线网络密钥重装漏洞(CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081、CVE-2017-13082、CVE-2017-13084、CVE-2017-13086、CVE-2017-13087、CVE-2017-13088），综合利用漏洞，远程攻击者利用该漏洞可能实现包括任意数据包解密和注入、TCP 连接劫持、HTTP 内容注入或单播和组寻址帧的重放攻击。漏洞危害程度为中危。

2 影响范围

漏洞影响的厂商如下：

Cisco

Google

HostAP

Peplink

OpenBSD

Fortinet.Inc

Red Hat.Inc

Aruba Networks

FreeBSD Project

Espressif Systems

Intel Corporation

Juniper Networks

Samsung Mobile

Microchip Technology

Microsoft Corporation

3 漏洞原理

WPA 全名为 Wi-Fi Protected Access，中文译名 Wi-Fi 网络安全接入，包括：WPA 和 WPA2 两个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统。WPA2 (WPA 第二版)是基于 WPA 的一种新的加密方式，具备完整的 IEEE 802.11i 标准体系。

WPA2 无线网络加密协议漏洞，入侵方式被称作“密钥重装攻击”。Wi-Fi 保护访问 II（WPA2）握手流量可以被操纵以引起随机数和会话密钥重用，导致无线接入点（AP）或客户端重新安装密钥。受影响的 AP 和客户端范围内的攻击者可能利用这些漏洞进行依赖于所使用的数据机密性协议的攻击。

4 修复建议

目前，已修复该漏洞的厂商如下，建议用户及时下载补丁进行更新：

- Cisco:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa
- Intel Corporation:

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00101&languageid=en-fr

- Juniper: http://kb.juniper.net/JSA10827
- Microsoft:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080
- Aruba:http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt
- Broadcom: Advisory will be distributed directly to customers
- Marvell: Advisory to be distributed directly to customers
- Mojo Networks: http://www.mojonetworks.com/wpa2-vulnerability
- Peplink:https://forum.peplink.com/t/security-advisory-wpa2-vulnerability-vu-228519/12715
- Sierra Wireless: https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin—wpa-and-wpa2-vulnerabilities/
- WatchGuard:https://www.watchguard.com/wgrd-blog/wpa-and-wpa2-vulnerabilities-update
- Wi-Fi Alliance: https://www.wi-fi.org/securityupdate2017。