# 对AirSnitch的审核和建议

## 目录

## 简介

本文档介绍对Airsnitch白皮书的回顾，以及可能的建议和措施。它适用于内部部署和云部署

## 摘要

2026年2月26日，研究人员发表了一篇题为《AirSnitch:Wi-Fi网络中消除客户隔离的神秘性和破坏客户隔离。” 在本文中，研究人员提出了绕过供应商对相同SSID内的无线客户端单播客户端隔离保护实施的方法。必须注意的是，提议的客户端隔离攻击是“内部攻击（恶意内部攻击）”，要求攻击者在发起攻击之前与无线基础设施相关联并通过身份验证。这些旁路方法并非由于无线规范或产品中的漏洞。无线网络中的加密方法也没有漏洞。这些攻击被视为机会性攻击，在部署了无线、交换和路由的最佳实践分层安全性的企业网络中，这些攻击可能无法成功。

AirSnitch攻击的主要目标是实现中间机器(MitM)位置，允许攻击者拦截、读取和修改受害客户端与Internet之间的流量，即使已启用客户端隔离也是如此。本研究将这些旁路分为三层：

- 共享密钥滥用：利用广播/组播密钥(GTK)在接入点上的基本服务集内的所有客户端之间共享这一事实。
- 路由层的注入攻击（网关反弹）：利用网络/IP层的ARP注入/MAC地址危害。
- 交换层（端口盗窃）：利用接入点(AP)和交换机的内部MAC学习行为。

在消费者/SOHO AP环境中，所有功能通常在单个设备（无线AP、交换机和第3层路由器）内运行，使设备容易出现配置错误或层间隔离不良。对于企业，每个供应商都有最佳的网络设计，可在网络的每一层使用零信任原则实现分段和隔离。

另请注意：在启用了重复MAC或IP地址检测等典型警报（大多数现代企业设备会报告和记录）的企业场景中，没有使用日志记录/警报或管理控制台。

这意味着这些内部攻击（特别是在企业情景中）是在未托管/未监控的网络中发起的，或者未将遥测配置为发送到安全控制台（安全事件和事件监控软件）的网络中发起的。

## 受影响的产品

针对思科无线接入点产品和Cisco Meraki无线产品(MR)，在接入点、无线控制器、交换和路由基础设施上未部署其他最佳实践安全配置时，针对企业无线接入点的攻击可能成功。

## 建议

为了降低本文档中概述的攻击可能性，思科建议在网络的每个层内使用最佳实践的深度防御。一般

指导和最佳实践摘要如下：

- 共享密钥滥用：共享密钥（单播或组）的滥用已经广为人知，因为漏洞是通过WPA2-Personal公开的。即使随着WPA3-Personal的出现，共享密钥的概念也会导致密钥的任何泄漏（分发、设备之间的共享、社会工程），不仅会危害SSID，而且会因为允许访问网络基础设施而影响到整个企业网络。如果要在企业中部署基于口令的网络，必须注意监控和分析连接到网络的设备。一旦密码短语/密码被发送给恶意内部人员后，设置“欺诈AP”以发起中间机器攻击就显得微不足道了。共享密钥网络(WPA2/WPA3-Personal)不能被视为“企业安全”，除非采取主动措施了解网络上的设备并采用其他分段技术（VLAN、VRF、交换矩阵、防火墙等）以及频繁轮换密码。

关于滥用共享IGTK，企业级无线网络中的遥测可以在使用共享IGTK看到WNM睡眠消息后发出警报。

思科还建议实施传输层安全以在可能的情况下加密传输中的数据，因为这会使攻击者无法使用获取的数据。

- 路由层的注入攻击（网关反射）和第2层端口盗窃：此攻击的前提是允许恶意内部人员路由第3层数据包（或影响BSS中其他设备的ARP表）。 具体而言，“我们发现攻击者可以发送数据包，目标IP地址是受害者的地址，目标MAC地址是网络网关的地址” — 企业级网络基础设施中存在多种机制，可缓解此类恶意活动并发出警报。企业推荐的第2层和第3层功能包括：

- DHCP监听：这可以防止攻击者欺骗DHCP服务器，并帮助构建合法IP/MAC对的绑定表。
- 动态ARP检测(DAI)：使用DHCP监听绑定表拦截和丢弃具有无效MAC到IP绑定的ARP数据包，从而防止MitM攻击的侦察阶段。
- 端口安全：限制单个物理端口（接入点上行链路）上允许的MAC地址数量，以防止攻击者使用伪造的MAC地址泛洪交换机。
- VLAN访问控制列表(VACL)/路由器ACL：明确拒绝源IP地址和目的IP地址都属于同一客户端子网的流量。这可确保路由器丢弃内部“发夹”流量，从而防止网关反弹。
- IP源保护(IPSG)：通过根据DHCP监听绑定数据库过滤流量来防止IP欺骗。如果攻击者尝试发送带有受害者所使用的IP地址的数据包，交换机会在入口端口将其丢弃。
- 单播反向路径转发(uRPF)：帮助确保到达接口的数据包来自合法的可到达源地址，从而缓解某些形式的IP欺骗。

# 结论

AirSnitch文章中的研究提醒我们，“客户端隔离”是一个局部功能，而非全面的安全边界。尽管研究人员成功证明了他们使用可能与供应商最佳实践不符的特定配置的旁路，但重要的是，将这些旁路归类为投机取巧的内部攻击，利用网络层之间缺乏安全配置，而不是802.11或Wi-Fi联盟中定义的无线加密协议的固有缺陷。

对于企业而言，主要优势是安全性不能依赖单一的“开/关”切换。当应用深度防御策略时，所识别的漏洞（例如网关退回和端口盗窃）会得到有效消除。通过从共享密钥环境（WPA2/3 — 个人）转向基于身份的身份验证（WPA3 — 企业），并实施强大的第2层和第3层保护(包括DHCP监听、动态ARP检测(DAI)、VACL以及设备强大的分段和分类)，组织可以确保客户端流量保持隔离，即使攻击者获得对SSID的验证访问权也是如此。

此外，研究人员企业测试案例中缺乏管理遥测技术，这突显了可见性的重要性。在托管的思科环境中，执行这些攻击所需的异常行为（如重复的MAC地址、IP欺骗或未经授权的WNM消息）会在安全事件和事件管理(SIEM)系统中立即触发警报。

# 最终建议

思科客户必须审核其无线部署，以确保他们应用了已建立的零信任架构。通过将无线安全与有线基础设施保护相集成，并保持主动监控，可以显着降低AirSnitch式攻击所带来的风险，从而确保安全且恢复力的网络环境。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。