默认网关IP地址指向无线客户端的ARP响应

目录

摘要

2019年，客户报告称，在给定子网中，默认网关IP地址的地址解析协议(ARP)响应间歇性地指向某些特定的无线客户端，而不是路由器。 对于同一VLAN/子网中的其他设备，这可能导致客户端或网络范围的连接问题。

条件

- 不正确的ARP响应指向运行10.14或更早版本的Apple macOS设备的MAC地址
- 运行2019年版Android的设备与同一子网相关联
- 与macOS设备关联的接入点是AP-COS（1800/2800/3800/4800/1540/1560/9100系列），在FlexConnect本地交换或SDA模式下，而不是Cisco IOS® AP。
- 接入点启用了FlexConnect代理ARP（ARP缓存） 默认情况下，FlexConnect ARP缓存在AP-COS 8.3及更高版本中启用8.2不易受攻击，因为它不支持AP-COS FlexConnect ARP缓存
- 此问题可能会影响使用AireOS或9800系列无线局域网控制器或Mobility Express的部署

根本原因

- 这不是恶意攻击，而是通过在休眠模式中的macOS设备与Android设备生成的特定广播流量之间的交互触发。 MacOS行为已在10.15及更高版本中修复
- 默认情况下，AP-COS AP在FlexConnect或SDA模式下提供代理ARP（ARP缓存）服务。由于它们的地址学习设计，它们将根据此流量修改表条目，从而修改默认网关ARP条目。

解决方法

禁用FlexConnect代理ARP（ARP缓存）。

- 如果运行带AireOS或Mobility Express的FlexConnect，请使用命令**config flexconnect arp-caching disable**
  此命令适用于8.10、8.9、8.8、8.5.151.0和8.5升级（8.5.140.13或更高版本）如果使用早期的8.5代码，则此命令不起作用(CSCvp73371)，因此请升级到8.5.151.0或更高版本如果使用8.3代码，请升级到8.3MR5升级（8.3.150.3或更高版本，可从TAC获得）以获取CSCvp73371 修复程序
- 如果将SDA交换矩阵模式与AireOS配合使用，请使用命令**config flexconnect arp-caching disable** 此命令适用于8.10、8.9.11.0、8.8.125.0和8.5.151.0如果使用早期的8.5或8.8代码，则此命令不起作用(CSCvk79850)，因此请升级到8.5.151.0 / 8.8.125.0 / 8.10或更高版本

- 如果使用9800系列控制器运行FlexConnect，请在无线配置文件flex下使用**no arp-caching**命令

通过禁用FlexConnect代理ARP，无线客户端的ARP请求将通过广播方式发送，而不是AP应答。这将在一定程度上增加无线手持设备（例如Cisco 8821电话）的电池消耗。

修复程序

如果运行带AireOS 8.10.120.0或更高版本的FlexConnect(CSCvp42721)或IOS-XE 17.2.1或更高版本，如果没有客户端需要使用静态寻址，则：

- 确保在每个位置所有AP都位于同一个非默认FlexConnect组中
- 在WLAN上配置所需的DHCP
- 使用命令**config flexconnect arp-caching enable**(AireOS)/**arp-caching**(IOS-XE)

这将防止客户端使用DHCP分配地址以外的IP地址。

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）。