預設網關IP地址指向無線客戶端的ARP響應

目錄

摘要

2019年，客戶報告，在給定子網中，預設網關IP地址的地址解析協定(ARP)響應間歇性地指向某些特定的無線客戶端，而不是路由器。 這可能導致同一VLAN/子網中的其他裝置出現客戶端或網路範圍的連線問題。

狀況

- 不正確的ARP響應指向運行10.14或更早版本的Apple macOS裝置的MAC地址
- 運行2019年版Android的裝置與同一個子網相關聯
- 與macOS裝置關聯的接入點是AP-COS（1800/2800/3800/4800/1540/1560/9100系列），在FlexConnect本地交換或SDA模式下，而不是Cisco IOS® AP。
- 存取點已啟用FlexConnect代理ARP（ARP快取） 預設情況下，在AP-COS 8.3及更高版本中啟用FlexConnect ARP快取8.2不易受攻擊，因為它不支援AP-COS FlexConnect ARP快取
- 此問題可能影響使用AireOS或9800系列無線LAN控制器或使用Mobility Express的部署

根本原因

- 這不是惡意攻擊，而是由macOS裝置在休眠模式下與由Android裝置生成的特定廣播流量之間的互動觸發。 MacOS行為已在10.15及更高版本中修正
- AP-COS AP在FlexConnect或SDA模式下預設提供代理ARP（ARP快取）服務。由於它們的地址學習設計，它們將根據此流量修改表條目，從而修改預設網關ARP條目。

因應措施

停用FlexConnect代理ARP（ARP快取）。

- 如果運行帶有AireOS或Mobility Express的FlexConnect，請使用命令**config flexconnect arp-caching disable**

  此命令適用於8.10、8.9、8.8、8.5.151.0和8.5升級（8.5.140.13或更高版本）如果使用早期的8.5代碼，則此命令不起作用(CSCvp73371)，因此請升級到8.5.151.0或更高版本如果使用8.3代碼，請升級到8.3MR5升級（8.3.150.3或更高版本，可從TAC獲得）以獲取CSCvp73371 修正
- 如果將SDA交換矩陣模式與AireOS配合使用，請使用命令**config flexconnect arp-caching disable** 此命令適用於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代碼，則此命令不起作用(CSCvk79850)，因此請升級到8.5.151.0 / 8.8.125.0 / 8.10或更高版本

- 如果使用9800系列控制器運行FlexConnect，請在**wireless profile flex**下使用**no arp-caching**命令

通過禁用FlexConnect代理ARP，無線客戶端的ARP請求將通過無線廣播，而不是AP應答。這將在一定程度上增加無線手持裝置（例如Cisco 8821電話）的電池消耗。

修正

如果運行帶有AireOS 8.10.120.0或更高版本的FlexConnect(CSCvp42721)或IOS-XE 17.2.1或更高版本，如果沒有客戶端需要使用靜態定址，則：

- 確保在每個位置，所有AP都位於同一個非預設FlexConnect組中
- 在WLAN上配置所需的DHCP
- 使用命令**config flexconnect arp-caching enable**(AireOS)**/arp-caching**(IOS-XE)

這將防止客戶端使用DHCP分配的IP地址以外的IP地址。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。