Date: June 16, 2026

Revision	Date	Changes
1.0	June 16, 2026	Initial release

CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N)
CVSSv4.0 Base Score: 5.3
(CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N)
Common Weakness Enumeration: CWE-653 (Insufficient Compartmentalization)

This vulnerability is being tracked by BUG 1787021

Description

The purpose of this advisory is to provide an announcement regarding potential vulnerabilities in Arista Access Points (APs) to the AirSnitch attacks published on February 26, 2026. This new class of attacks devices bypass mechanisms by which client isolation can be broken in Wi-Fi networks. The attacks can only be carried out by a client that is legitimately connected to the network through a Guest Service Set Identifier (SSID) or by a malicious insider. These attacks cannot be launched by devices external to the enterprise network.

The AirSnitch threat model includes traffic injection by the attacker to other clients and interception of a client's uplink/downlink traffic, leading to fully bi-directional Machine-in-the-Middle (MitM) attacks. The attacker can exploit vulnerabilities across three operational layers:

1. **Wi-Fi Encryption Layer:** The attacker misuses the Group Temporal Key (GTK) obtained during the standard 4-way handshake. By manipulating frame addressing over the air, the attacker bypasses the AP's client isolation protections.
2. **Internet Protocol (IP) Routing Layer:** The attacker injects packets leveraging Layer 2 (L2) and Layer 3 (L3) destination address inconsistencies, forcing the local Gateway to reflect ("bounce") traffic to a victim client. This Gateway Bouncing can potentially allow an attacker on an isolated Guest SSID to reach devices on a Corporate SSID.
3. **Link/Switching Layer:** The attacker impersonates a victim's Media Access Control (MAC) address across a different Basic Service Set Identifier (BSSID). By flooding frames, the attacker manipulates the MAC-to-port forwarding tables on the access point, effectively stealing the victim's logical port.

Executive Risk Summary: Although the CVSS v3.1 score is classified as High because a successful exploit can cross security boundaries to impact separate systems (Scope Changed - S:C), the real-world risk is significantly minimized by strict operational requirements. An external threat actor cannot execute this attack; an attacker must already possess valid network credentials or legitimate access to an adjacent wireless SSID (such as a Guest or Corporate network).

Vulnerability Assessment

Affected Software

- None

Note: this is an architectural configuration dependency rather than an issue with the product itself.

Affected Platforms

The attacks devised to bypass client isolation can be effective against all Arista Access Points if they are not configured with recommended security best practices mentioned under the Mitigation section in this advisory.

Required Configuration for Exploitation

In order to be vulnerable to the AirSnitch attack, the attacker must be legitimately connected to the network through a guest SSID or must be a malicious insider.

Indicators of Compromise

The following are potential indicators of Compromise:

A. Potential Signs of Active Exploitation (High Alert)

- **MAC Address Impersonation (Port Stealing):** The same MAC address appearing simultaneously from multiple distinct network locations, different APs, or varying switch interfaces.

  Rapid MAC-to-Port Fluctuations: Sudden, high-frequency MAC relearning events recorded in switch/AP system logs.

  ARP Poisoning/Spoofing Signals: Multiple distinct Address Resolution Protocol (ARP) replies detected for a single IP address, or an anomalous influx of frequent gratuitous ARPs.

  Cryptographic Disruptions: End-users reporting sudden Transport Layer Security (TLS) certificate warnings or unexpected session interruptions.

B. Signs of an Insecure / Vulnerable Network State

- **Unexpected Client-to-Client Communication:** A client on an supposedly "isolated" SSID successfully initiating ICMP Pings, exchanging direct data packets, or receiving forwarded traffic from another local client.

  Gateway Bouncing Behaviors: Same-subnet traffic needlessly traversing the local gateway/router interface, or observable "hairpin" forwarding actions.

Broadcast/Multicast Abuse: Excessive broadcast volume or unexpected multicast propagation reaching isolated client boundaries.

Mitigation

- **Mitigating GTK abuse**
  Enforce WPA3-Enterprise using Protected Management Frames (PMF) or implement 802.1X authentication where unique pairwise keys are systematically rotated, minimizing reliance on static, shared infrastructure keys.
- **Mitigating Gateway bouncing & Port stealing**
  Enterprise-level network infrastructures provide several defensive tools designed to detect and prevent a malicious insider routing network layer traffic or training AP's ARP tables. Customers are advised to enable the below features to protect their networks:

    - Source port filtering: Source port filtering prevents packets from egressing the same interface they ingressed on. This blocks "hairpin" traffic generated in Gateway bouncing type of attacks.
    - IP Locking: IP Locking provides Layer 2 port-level security by validating MAC-IP bindings and blocking rogue DHCP traffic.
    - Port Security: Restricts the volume of MAC addresses permitted on an individual physical port to block attackers from overwhelming the switch with spoofed MAC addresses. It prevents unauthorized devices from forwarding packets by dynamically learning and enforcing a configurable MAC address limit per interface.
    - VLAN Access Control Lists (VACLs) / Router ACLs: Explicitly deny traffic where both the source and destination IP addresses belong to the same client subnet. This prevents Gateway Bouncing by ensuring the router drops internal "hairpin" traffic.
    - IP Source Guard: IP Source Guard (IPSG) is a Layer 2 security feature that prevents IP spoofing attacks by filtering inbound IP packets based on source MAC and IP address validation against configured binding entries. IPSG effectively blocks IP spoofing attempts by dropping packets at the ingress port if the source IP does not match the verified victim's address.
    - Unicast Reverse Path Forwarding (uRPF): By verifying that packets entering an interface originate from a valid and reachable source address, uRPF serves as a critical defense against various forms of IP spoofing.

Note: POTENTIAL SERVICE DISRUPTION: Enabling Layer 2 security features such as Port Security, IP Source Guard, and Dynamic ARP Inspection (DAI) on active production switch ports can cause immediate link disruption if legitimate clients violate unconfigured binding rules. Ensure these policies are validated in a staging environment prior to global deployment.

Apply the following foundational hardening configurations to the upstream switch infrastructure hosting your Arista Access Points:

1. **Configure IP Source Guard (IPSG) & DHCP Snooping**

```
ip dhcp snooping
ip dhcp snooping vlan <VLAN-IDs>
!
interface <Interface_to_APs>
    ip verify source
```

To verify whether DHCP snooping is enabled, the following commands can be used:

```
show ip dhcp snooping
show ip verify source detail
```

2. **Enforce Port Security Constraints**

```
interface <Interface_to_APs>
   switchport port-security
   switchport port-security mac-address maximum 32
   switchport port-security violation protect
```

3. **Prevent Gateway Bouncing via Router ACLs**

```
ip access-list deny_hairpin
   10 deny ip <Client_Subnet_CIDR> <Client_Subnet_CIDR>
   20 permit ip any any
!
interface vlan <VLAN-ID>
   ip access-group deny_hairpin in
```

Resolution

Because the AirSnitch exploit vectors target cross-layer architectural design parameters rather than a specific code defect or software regression, there is no separate software patch or software release associated with this advisory. The client isolation bypass methods exploited in AirSnitch attacks are possible only for malicious insiders. The mitigation strategies mentioned above can successfully circumvent the attacks, and protect the network from the attacks.

Hotfix

No hotfixes are available for this issue.

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support