Grandstream Networks, Inc.

# AirSnitch: Wi-Fi Client Isolation Risks and Recommended Network Hardening

# AirSnitch: Wi-Fi Client Isolation Risks and Recommended Network Hardening

AirSnitch describes a group of Wi-Fi attacks that can bypass client-isolation controls and expose traffic between wireless clients that should remain separated. This guide follows the vulnerability structure and mitigation guidance supplied for Grandstream GWN wireless deployments and adds verified interface examples for easier implementation.

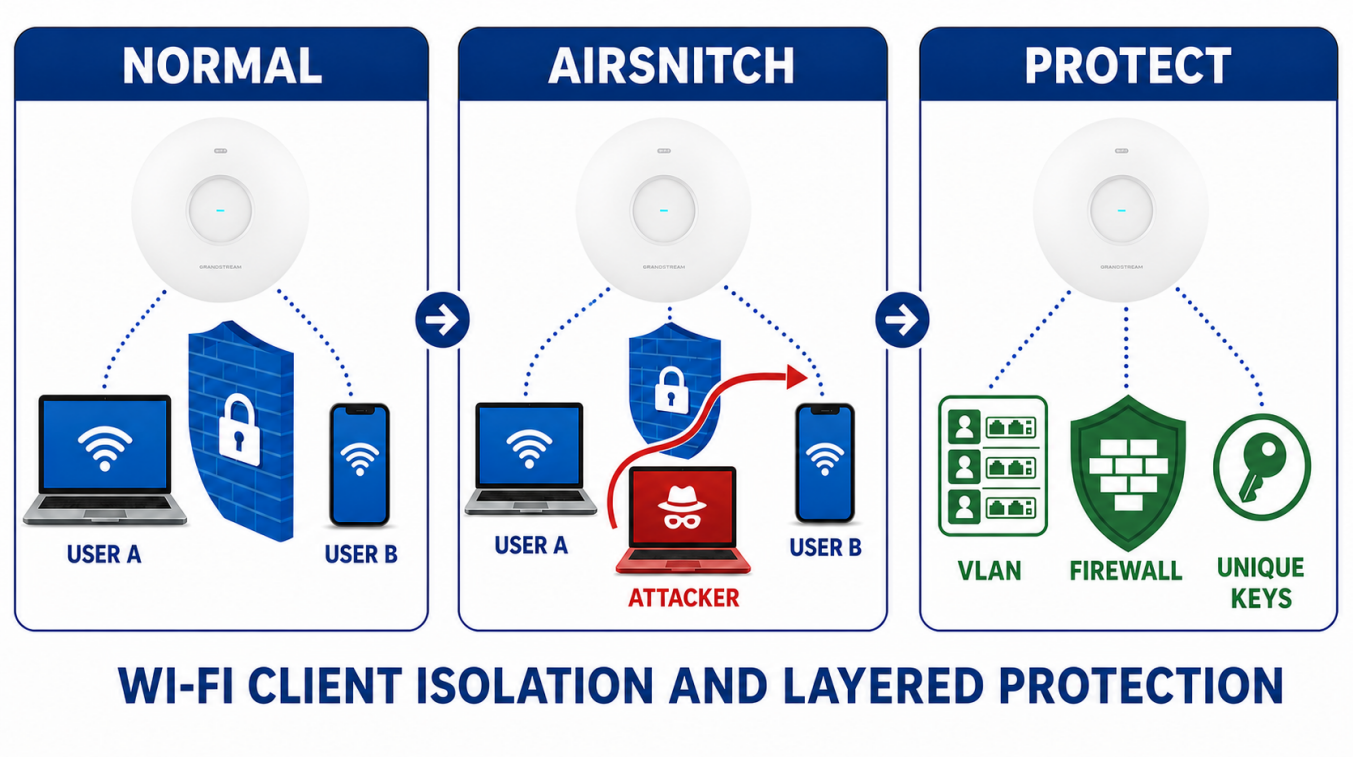
**Scope note**

This is defensive hardening guidance, not a Grandstream vulnerability advisory or a confirmed affected-model list. Feature availability and menu names can vary by model, firmware, and management platform.

## 1. Background

On February 23, 2026, researchers from the University of California, Riverside and KU Leuven presented AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks at the Network and Distributed System Security Symposium (NDSS). The research describes Wi-Fi techniques that can bypass certain isolation controls and create risks including denial of service, unauthorized frame injection, traffic modification, traffic redirection, and unauthorized access.

The attack scenarios assume that the attacker can join the target Wi-Fi network, typically by possessing a valid pre-shared key (PSK). An open network already allows access without a PSK and is therefore outside the scope of this guide. Without access to the WLAN, these attacks cannot be launched as described.




*AirSnitch targets assumptions around Wi Fi client isolation layered controls help limit the attack path and impact*

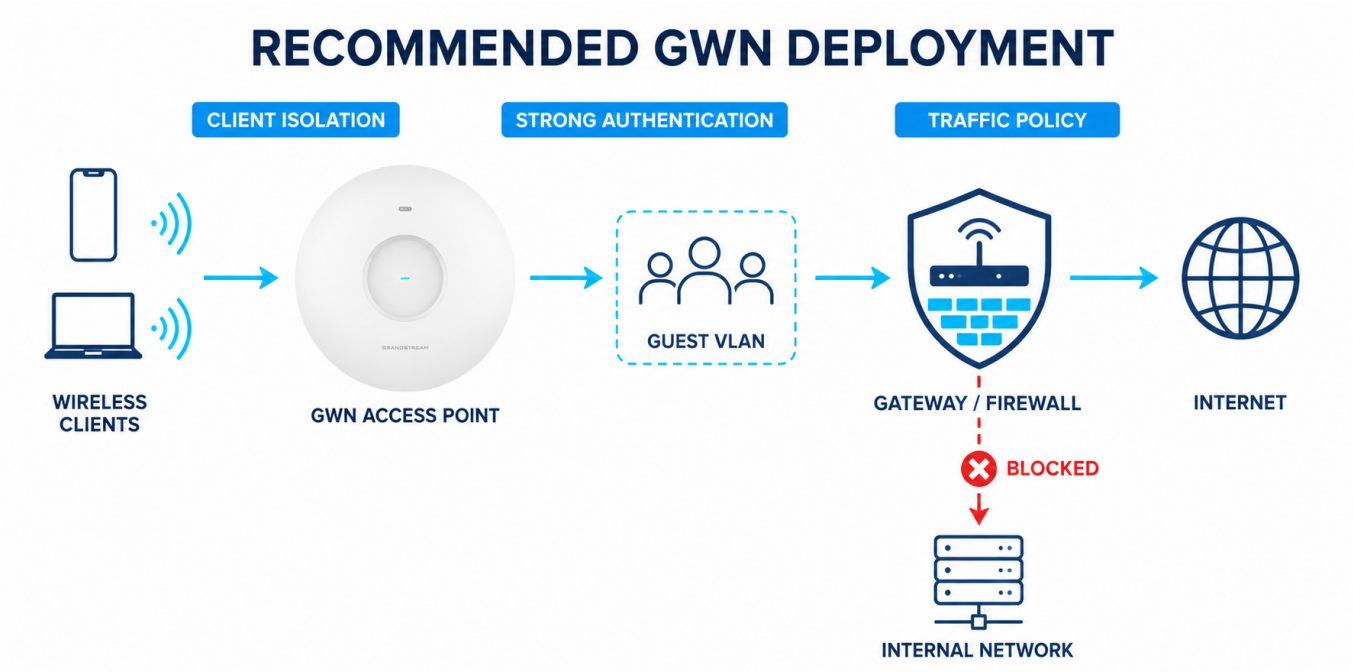
## 2. Handling Suggestions

Organizations should treat wireless security as a layered network design. Authentication, wireless isolation,

switching protections, routing policy, multicast controls, monitoring, current firmware, and end-to-end encryption work together; no single option should be treated as the complete security boundary.

## 2.1 Common Network Security Protection Measures

| No. | Security measure | Purpose |
|---|---|---|
| 1 | User-access authentication, such as 802.1X | Controls network access and helps prevent unauthorized client connections. |
| 2 | Layer 2 and Layer 3 user isolation | Restricts direct communication between users on the same subnet or across routed segments. |
| 3 | Port isolation | Separates physical or logical switch ports to reduce lateral movement. |
| 4 | Policy-based routing (PBR) | Controls forwarding paths according to policy rather than only the standard routing table. |
| 5 | IP Source Guard (IPSG) | Uses DHCP snooping and binding information to reject traffic with forged source IP or MAC addresses. |
| 6 | ARP inspection and attack protection | Rejects ARP packets whose MAC-to-IP mapping does not match trusted bindings, reducing man-in-the-middle risk. |
| 7 | URL filtering | Limits the destinations that users can access according to organizational policy. |
| 8 | WPA3 with PPSK or 802.1X | Avoids one network-wide shared credential and reduces exposure when an individual password is disclosed. |
| 9 | Multicast-to-unicast and multicast suppression | Reduces unnecessary shared group traffic and related GTK-based multicast injection paths. |
| 10 | Tunnel forwarding with user isolation | Restricts cross-user and cross-segment redirection or interception at Layers 2 and 3. |
| 11 | Rogue AP detection | Detects suspicious APs and helps prevent clients from connecting to attacker-controlled infrastructure. |




*Example defense in depth path for a guest or untrusted GWN SSID*

# 3. AirSnitch Vulnerability Details

## 3.1 Shared GTK Frame Injection

**Official CVE record:** CVE-2026-23601

**Vulnerability description**

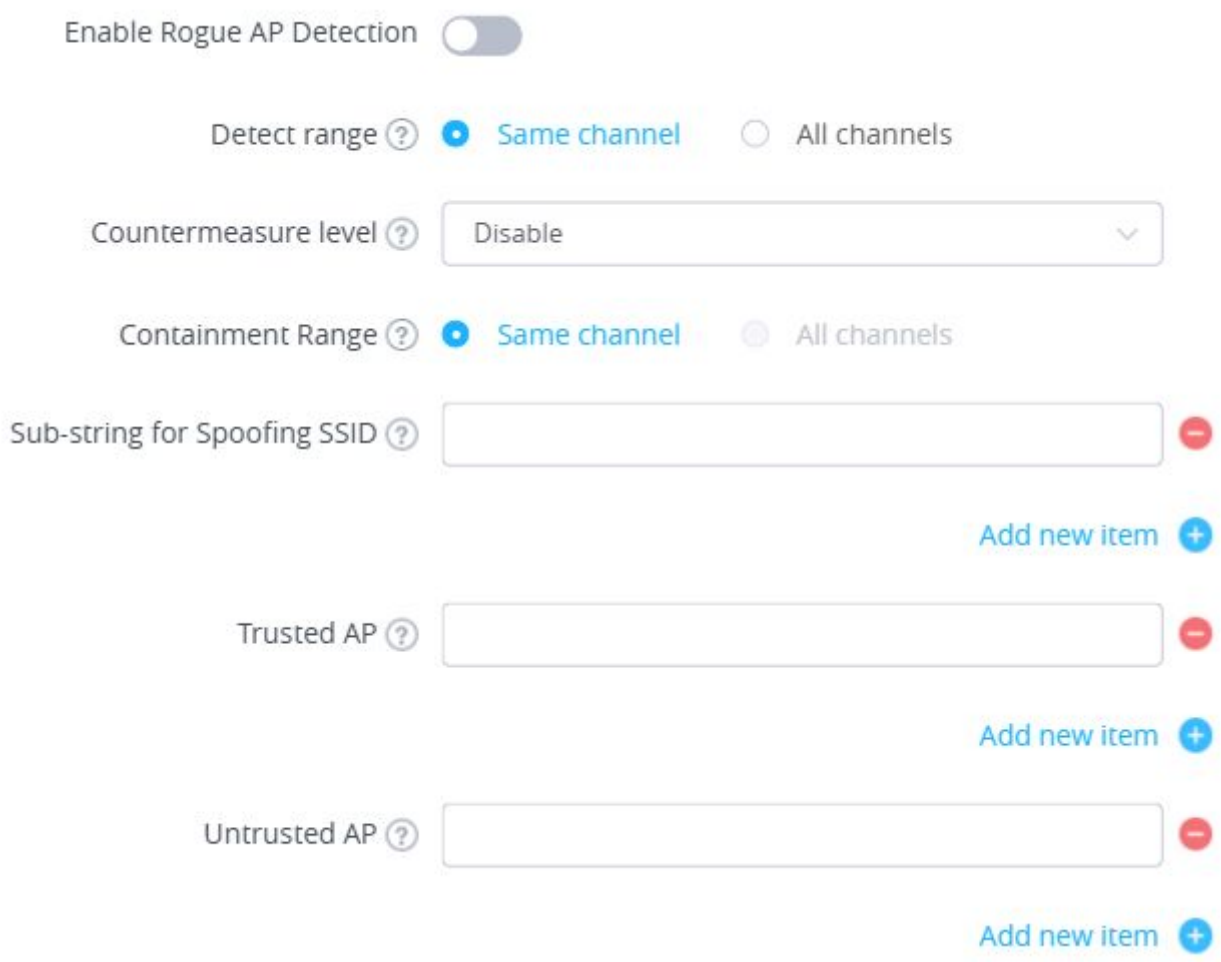
An attacker impersonating the primary BSSID may forge frames encrypted with the shared Group Temporal Key (GTK) and include a chosen payload. If successful, modified data can be delivered to a specific wireless client, bypassing the isolation normally expected from Wi-Fi encryption.

**Recommended mitigation**

- Use WPA3 with Private Pre-Shared Key (PPSK) or 802.1X authentication so users do not depend on one network-wide credential.
- Use Rogue AP detection to identify suspicious radios and reduce the chance of clients connecting to an attacker-controlled AP.

**GWN configuration**

Security > Rogue AP




*Rogue AP controls in a Grandstream GWN access point interface Configure detection and containment according to the site wireless security policy*

## 3.2 GTK-Based Client Isolation Bypass

**Official CVE record:** CVE-2026-23808

**Vulnerability description**

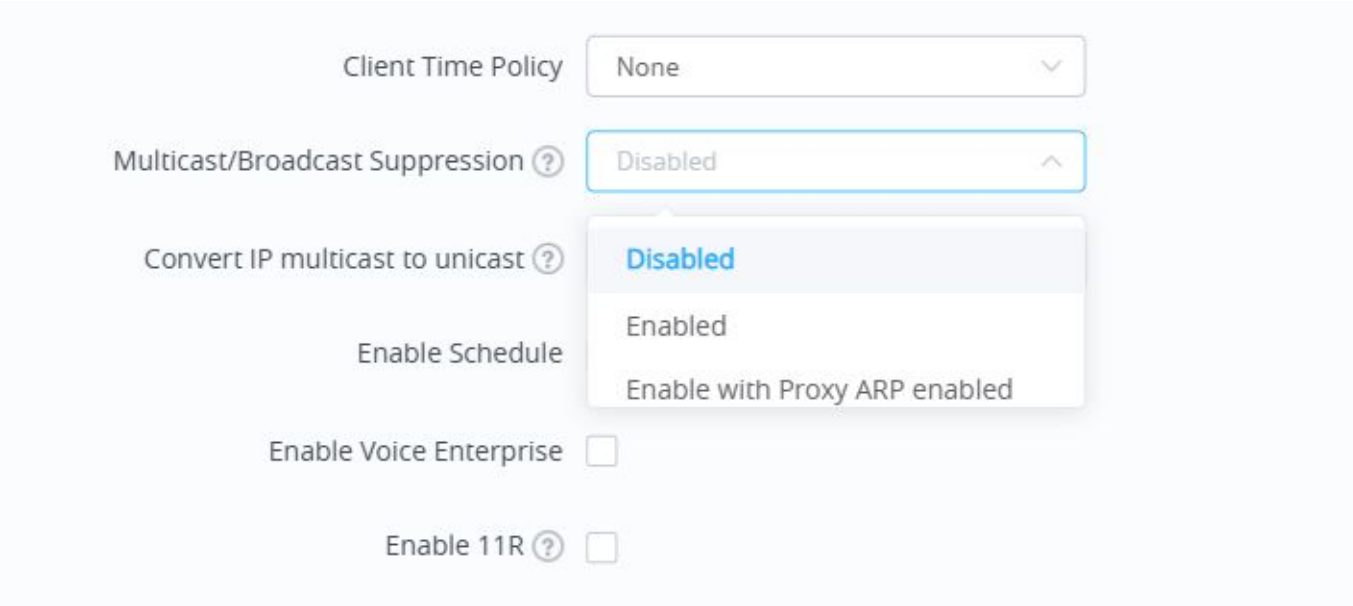
This vulnerability can allow a malicious client to influence the GTK installed on another client. A successful attack may enable unauthorized frame injection, bypass client isolation, interfere with traffic between clients, and weaken network segmentation, integrity, and confidentiality.

**Recommended mitigation**

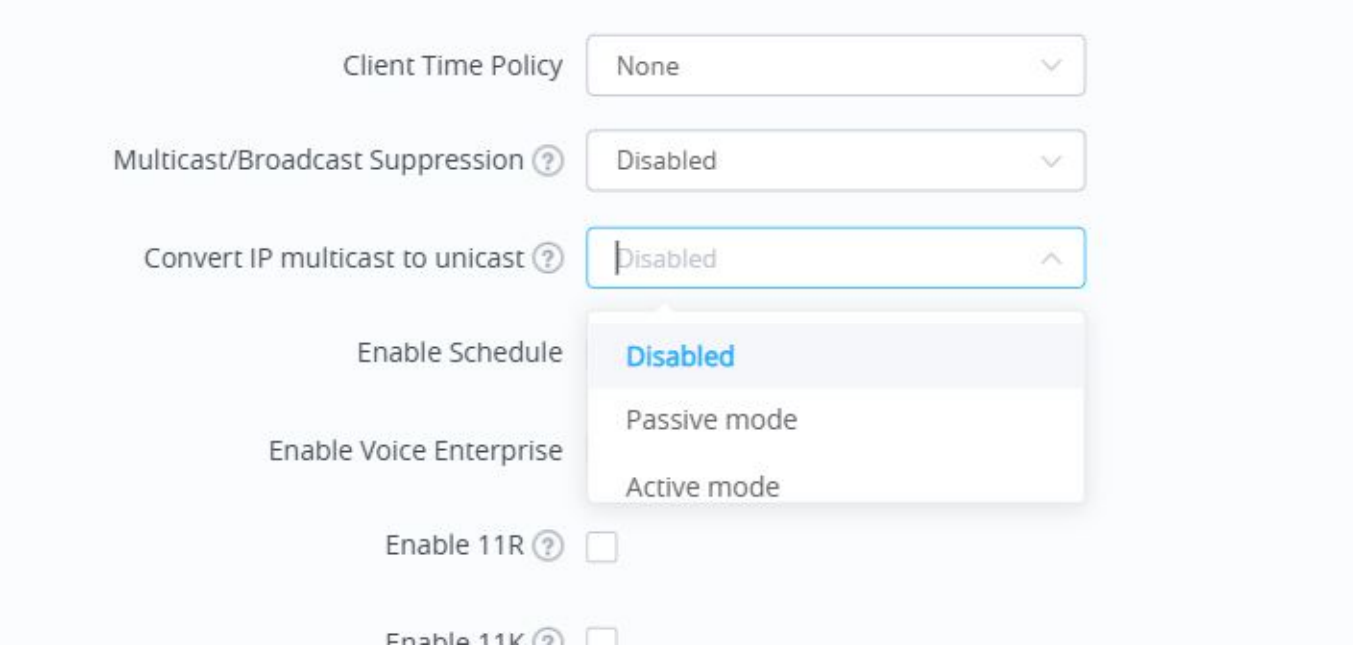
Where compatible with required services, enable multicast-to-unicast conversion and multicast/broadcast suppression. Test casting, printing, voice, IoT discovery, and other multicast-dependent applications before broad deployment.

**GWN configuration**

Wi-Fi > SSID > Edit SSID > Advanced




*MulticastBroadcast Suppression options*




*Convert IP multicast to unicast options*

## 3.3 Cross-BSSID Isolation Bypass and Traffic Redirection

**Official CVE record:** CVE-2026-23809

**Vulnerability description**

An attacker may forge a legitimate client MAC address and exploit the relationship between BSSIDs and their associated virtual ports. Packets intended for the legitimate client can then be redirected to the attacker, creating risks such as eavesdropping, session hijacking, or denial of service.

**Recommended mitigation**

Enable IP Source Guard (IPSG) where it is supported in the deployment. IPSG should use trusted DHCP snooping and binding information to reject traffic with a forged source IP or MAC address.

**GWN configuration**

Wi-Fi > SSID > Edit SSID > Advanced > IP Source Protection

## 3.4 Cross-BSSID GTK Re-encryption and Traffic Injection

**Official CVE record:** CVE-2026-23810

**Vulnerability description**

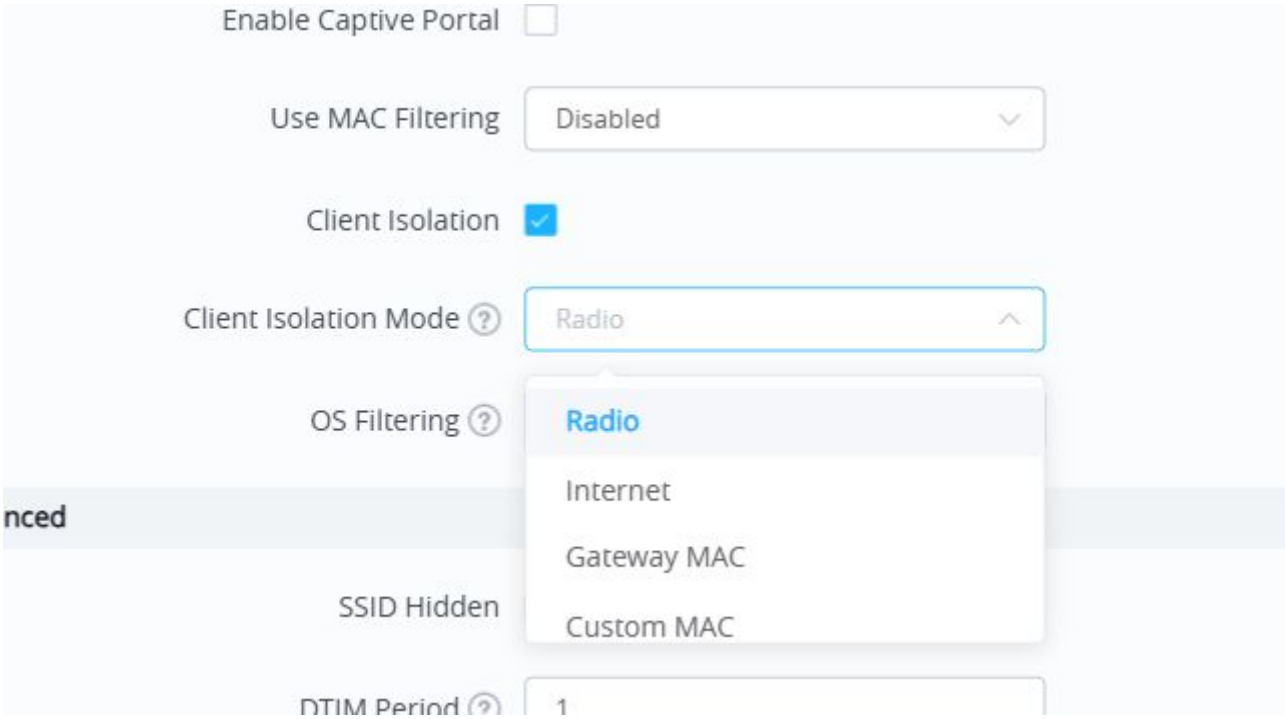
An authenticated attacker may construct malicious Wi-Fi frames that the AP classifies as multicast traffic and re-encrypts with the GTK associated with the victim BSSID. When combined with port-stealing techniques, this can support traffic injection, redirection, or man-in-the-middle attacks across BSSIDs.

**Recommended mitigation**

Enable Client Isolation and select the mode that matches the intended WLAN policy. Reinforce it with VLAN segmentation and explicit gateway or firewall restrictions.

**GWN configuration**

Wi-Fi > SSID > Edit SSID > Advanced > Client Isolation




*In the Grandstream GWN access point interface enable Client Isolation and choose the mode that matches the intended WLAN policy*

## 3.5 Layer 2/Layer 3 Traffic Interception

**Official CVE record:** CVE-2026-23811

**Vulnerability description**

An attacker may bypass Layer 2 communication restrictions between clients and redirect traffic at Layer 3. A successful exploit can enable a bidirectional man-in-the-middle attack.

**Recommended mitigation**

- When using tunnel forwarding, enable user isolation.
- If attacker and victim are on different network segments, apply policy-based routing and gateway/firewall rules that restrict inter-segment communication.
- If both are on the same subnet, enforce Layer 2 isolation at the gateway or switching layer.

### 3.6 Routing-Node Impersonation

**Official CVE record:** CVE-2026-23812

**Vulnerability description**

A standard wired or wireless client may use address-forgery techniques to impersonate a gateway. If successful, the attacker can redirect, intercept, or modify traffic that should have been sent to the legitimate network gateway.

**Recommended mitigation**

Enable IP Source Guard (IPSG) or the equivalent IP Source Protection feature where supported, and reinforce it with trusted DHCP bindings, ARP inspection, and restrictive gateway policy.

**GWN configuration**

Wi-Fi > SSID > Edit SSID > Advanced > IP Source Protection

**Validation reminder:** After applying changes, test authorized clients across radios, BSSIDs, APs, VLANs, and roaming paths. Confirm that required Internet, DHCP, DNS, portal, voice, casting, printing, and discovery services still work while unauthorized client-to-client and internal-network access remains blocked.

## 4. Supported GWN Wireless Products

This guidance applies at the product-family level only where the installed model and firmware expose the relevant wireless security controls.

| Product family | How this guidance applies |
|---|---|
| **GWN76xx Access Points** | Apply the recommendations supported by the installed model, firmware, and management mode. |
| **GWN70xx Wireless Routers** | Apply the recommendations only on models that provide Wi-Fi SSIDs and equivalent isolation or traffic-policy controls. |

## 5. References


- CVE-2026-23601 - Shared GTK Frame Injection
- CVE-2026-23808 - GTK-Based Client Isolation Bypass
- CVE-2026-23809 - Cross-BSSID Isolation Bypass and Traffic Redirection
- CVE-2026-23810 - Cross-BSSID GTK Re-encryption and Traffic Injection
- CVE-2026-23811 - Layer 2/Layer 3 Traffic Interception
- CVE-2026-23812 - Routing-Node Impersonation
- NDSS Symposium: AirSnitch-Demystifying and Breaking Client Isolation in Wi-Fi Networks


---

Review all settings against the organization's network design and the documentation for the exact product

and firmware in use. Perform security testing only on networks and devices you are authorized to assess.