INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 06:38 UTC

AirSnitch Breaks Wi-Fi Client Isolation Across All Encryption Standards, Enterprise MitM Now Viable Without Breaking Crypto

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0076
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	WPA2/WPA3-Enterprise protocol implementations (broad); wpa_supplicant; hostapd; Android, macOS, iOS, Windows, Ubuntu Linux; Netgear, D-Link, Ubiquiti, Cisco, DD-WRT, OpenWrt access points
Published	2026-04-22T10:00:22+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

AirSnitch, disclosed at NDSS 2026, demonstrates a class of Wi-Fi attacks that bypasses client isolation on WPA2 and WPA3-Enterprise networks without decrypting a single packet, the attack subverts network architecture assumptions at the protocol level, making encryption an insufficient control on its own. Every major client operating system (Windows, macOS, iOS, Android, Ubuntu Linux) and access points from Netgear, D-Link, Ubiquiti, Cisco, and others are confirmed affected, placing enterprise wireless infrastructure broadly at risk. This is not a cryptographic weakness that vendors can patch quietly; it signals that organizations treating WPA2/3-Enterprise as a client isolation boundary need to re-evaluate that assumption structurally and apply supplemental controls immediately.

Technical Analysis

AirSnitch describes a class of machine-in-the-middle (MitM) attacks operating at OSI Layers 1 and 2, below the cryptographic layer, that defeat the client isolation guarantees enterprises rely on in WPA2 and WPA3-Enterprise deployments. Presented at the Network and Distributed System Security Symposium (NDSS 2026) and covered in depth by Palo Alto Networks Unit 42, the attack achieves full bidirectional interception of traffic between wireless clients without requiring the attacker to break or bypass encryption. The mechanism exploits low-level protocol interactions in the 802.11 frame handling and client association logic implemented by wpa_supplicant and hostapd, the open-source components that underpin Wi-Fi authentication across virtually all

major operating systems and access point firmware.

The attack's power lies precisely in what it doesn't do. Because AirSnitch does not touch the cryptographic layer, detection approaches and defenses that focus on cryptographic integrity, certificate validation, encrypted transport, or WPA3's stronger authentication handshake, provide no protection. The attacker positions between two clients, or between a client and the upstream gateway, intercepting and optionally modifying traffic at the frame level before encryption is even applied or after it is processed by the intended recipient's stack. This maps directly to MITRE ATT&CK T1557 (Adversary-in-the-Middle) and its sub-techniques T1557.002 (ARP Cache Poisoning) and T1557.004, as well as T1040 (Network Sniffing) and T1565 (Data Manipulation).

The affected surface is unusually broad. Unit 42 confirmed impact across Android, macOS, iOS, Windows, and Ubuntu Linux on the client side, and across access points from Netgear, D-Link, Ubiquiti, Cisco, DD-WRT, and OpenWrt. No CVE has been assigned as of this report, which reflects the architectural nature of the vulnerability, it is not a single implementation bug in a single product but a class of weaknesses (CWE-300, CWE-290, CWE-345, CWE-923, CWE-311) rooted in protocol design assumptions that do not hold at Layer 1/2.

For enterprise security teams, the critical implication is architectural. Organizations that have deployed WPA2/3-Enterprise and assumed that client isolation, the property that prevents wireless clients from communicating directly with or intercepting traffic from other clients, is enforced by the protocol must revise that assumption. Supplemental controls at Layers 3 and above, including 802.1X port-based access control, dynamic VLAN assignment per client, micro-segmentation, and application-layer encryption (TLS everywhere), become the effective perimeter. The attack also highlights the risk of shared wireless environments: guest networks, BYOD segments, and conference Wi-Fi that share physical infrastructure with enterprise traffic are particularly exposed if network isolation relies solely on SSID or VLAN separation without additional enforcement.

Action Checklist

1. Step 1: Assess exposure, audit all enterprise wireless deployments for reliance on WPA2/3-Enterprise as the sole client isolation control; include guest, BYOD, IoT, and conference SSIDs in scope; document which access point vendors (Netgear, D-Link, Ubiquiti, Cisco, DD-WRT, OpenWrt) are in use and flag them for firmware monitoring
2. Step 2: Review controls, verify that 802.1X port-based access control and dynamic per-client VLAN assignment are enforced; confirm that application-layer TLS is required for all sensitive traffic traversing wireless segments, and that zero-trust network access (ZTNA) or micro-segmentation policies are not solely dependent on Layer 2 isolation
3. Step 3: Update threat model, add Layer 1/2 MitM via AirSnitch-class attacks (T1557, T1557.002, T1557.004, T1040) to your wireless threat register; treat shared physical wireless infrastructure as an untrusted medium regardless of encryption standard in use
4. Step 4: Communicate findings, brief leadership that WPA3-Enterprise does not eliminate wireless MitM risk; frame the issue as an architectural gap, not a patch-and-done vulnerability; connect the risk to specific high-value environments (executive areas, R&D segments, financial systems on Wi-Fi)
5. Step 5: Monitor developments, track Unit 42, NDSS 2026 paper publication, and affected vendor advisories (Cisco, Ubiquiti, Netgear, D-Link) for firmware updates, protocol-level mitigations, or updated guidance from CISA; no patch currently addresses the root protocol design issue

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if Kismet, AP syslog, or RADIUS accounting logs show unexpected client-to-client traffic on isolation-enforced SSIDs in segments hosting PII, PHI, PCI-DSS cardholder data, or executive communications — any confirmed or suspected AirSnitch-class lateral traffic in these segments triggers breach notification assessment obligations under HIPAA §164.312(e), PCI-DSS Requirement 12.10, and applicable state breach notification laws.
Recovery Notes	Because AirSnitch is a protocol-design weakness with no available patch, recovery is architectural: validate that per-client dynamic VLAN assignment is confirmed active on all affected AP vendors (Cisco, Ubiquiti, Netgear, D-Link) and that application-layer TLS mutual authentication is enforced for all sensitive services accessible from wireless segments — these are your primary compensating controls. Monitor RADIUS accounting logs and AP association logs daily for 30 days post-control implementation to establish a new behavioral baseline, watching for anomalous VLAN assignments or unexpected client-to-client ARP traffic that would indicate the compensating controls are misconfigured. Revisit the threat model and compensating control adequacy when the NDSS 2026 paper is formally published or when any affected vendor releases a firmware advisory, as the full exploitation technique details may expand the known attack surface.
Forensic Artifacts	RADIUS accounting logs (FreeRADIUS: /var/log/freeradius/radacct//detail-) — fields Calling-Station-Id (client MAC), Tunnel-Private-Group-Id (assigned VLAN), and NAS-Port-Id (AP radio) will show whether a client that should be isolated was assigned to a shared VLAN, which is the network-layer precondition AirSnitch exploits | AP syslog output for 802.11 client association events — on Cisco WLC: 'debug client ' captures; on Ubiquiti UniFi: /var/log/messages on the AP containing 'assoc' and 'auth' events — unexpected client MAC associations on isolation-enforced SSIDs immediately before anomalous traffic are the earliest forensic indicator of a staged AirSnitch attack | Kismet or Wireshark pcap captures in monitor mode on the affected wireless channel — filter for 802.11 data frames with both source and destination MACs belonging to clients on the same SSID; under correct client isolation, direct client-to-client 802.11 frames should not appear, so their presence in a pcap is direct forensic evidence of isolation bypass | ARP table snapshots from wireless-connected hosts at the time of suspected exploitation — on Windows: 'arp -a > arp_snapshot.txt'; on Linux/macOS: 'arp -n > arp_snapshot.txt' — AirSnitch-class MitM may manifest as unexpected ARP entries mapping legitimate gateway IPs to attacker-controlled MAC addresses, which is the Layer 2 artifact of T1557.002 (ARP Cache Poisoning) within the attack chain | wpa_supplicant debug logs from affected client endpoints (Linux: 'wpa_supplicant -d -D nl80211 -i wlan0 -c /etc/wpa_supplicant.conf' output; Android: bugreport wireless section; Windows: 'netsh wlan show all' and Event Viewer > Applications and Services Logs > Microsoft > Windows > WLAN-AutoConfig > Operational, Event ID 8001/8003 for association events) — these logs capture the EAP authentication exchange and PMKID/GTK negotiation details that confirm which encryption standard was in use at time of suspected exploitation

Per-Action IR Details

Step 1: Assess exposure — audit all enterprise wireless deployments for reliance on WPA2/3-Enterprise as the sole client isolation control; include guest, BYOD, IoT, and conference SSIDs in scope; document which access point vendors (Netgear, D-Link, Ubiquiti, Cisco, DD-WDD, OpenWrt) are in use and flag them for

firmware monitoring

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and inventorying assets/controls before an incident occurs

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires knowing which assets and controls are in scope before containment actions are possible, NIST SI-4 (System Monitoring) — identify which wireless segments lack compensating monitoring controls beyond Layer 2 isolation, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — enumerate all APs by vendor (Netgear, D-Link, Ubiquiti, Cisco, DD-WRT, OpenWrt) with firmware versions, SSID configuration, and client isolation setting, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — flag all identified AP vendors for firmware advisory tracking given no patch currently resolves the AirSnitch protocol-level design issue

Compensating: Run 'iwlist scan' or 'iw dev wlan0 scan' from a Linux host on each wireless segment to enumerate visible SSIDs and BSSID/vendor OUI combinations; cross-reference OUIs against the IEEE OUI registry (standards-oui.ieee.org) to map vendor presence without enterprise NAC. For AP inventory where SNMP is available, use 'snmpwalk -v2c -c public 1.3.6.1.2.1.1' to pull sysDescr and firmware strings. Build a spreadsheet mapping each SSID to: vendor, firmware version, client isolation setting (enabled/disabled), and VLAN assignment — this is your exposure baseline.

Evidence: Before auditing, capture current AP configuration exports (Cisco: 'show running-config' via SSH; Ubiquiti UniFi: Settings > System > Backup; Netgear/D-Link: admin UI config export) as timestamped snapshots. Preserve RADIUS server logs showing which client MACs authenticated to each SSID within the last 30 days — on FreeRADIUS, these are in /var/log/freeradius/radius.log with Auth-Type and Called-Station-Id fields identifying the SSID. This baseline is your pre-incident evidence that client isolation was (or was not) the sole isolation control at time of potential exploitation.

Step 2: Review controls — verify that 802.1X port-based access control and dynamic per-client VLAN assignment are enforced; confirm that application-layer TLS is required for all sensitive traffic traversing wireless segments, and that zero-trust network access (ZTNA) or micro-segmentation policies are not solely dependent on Layer 2 isolation

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: validating that preventive and detective controls are correctly configured prior to exploitation

Controls: NIST SC-8 (Transmission Confidentiality and Integrity) — verify TLS is enforced at the application layer for all sensitive wireless traffic because AirSnitch demonstrates Layer 2 encryption alone is insufficient against MitM on shared wireless infrastructure, NIST AC-17 (Remote Access) — confirm 802.1X authentication with dynamic VLAN assignment is active; static VLAN assignment without per-session enforcement leaves clients on shared broadcast domains exploitable by AirSnitch-class traffic injection, NIST SI-7 (Software, Firmware, and Information Integrity) — validate that ZTNA/micro-segmentation policy enforcement points are upstream of the wireless segment and do not trust Layer 2 client isolation assertions from the AP, CIS 4.4 (Implement and Manage a Firewall on Servers) — confirm server-side firewall rules do not implicitly trust traffic sourced from wireless VLANs without application-layer authentication, CIS 6.3 (Require MFA for Externally-Exposed Applications) — application-layer controls must authenticate the client identity independently, since AirSnitch allows an attacker to impersonate or intercept a legitimate isolated client's traffic at Layer 2

Compensating: For 802.1X verification without NAC tooling: on a Cisco WLC, run 'show client detail ' to confirm VLAN assignment per authenticated client; on Ubiquiti UniFi, check Client Properties in the controller UI for 'VLAN' field. To verify TLS enforcement without a proxy: run 'ssldump -i -n' or Wireshark with display filter 'tcp.port == 80 && wlan' on a monitor-mode interface — any cleartext HTTP from wireless clients is a finding. For ZTNA gap assessment with no budget: deploy Nginx with mutual TLS (mTLS) as a reverse proxy in front of internal services on Wi-Fi-accessible segments to enforce application-layer identity independent of Layer 2.

Evidence: Capture RADIUS accounting logs showing VLAN assignments per session (FreeRADIUS: /var/log/freeradius/radacct//detail-, fields: Tunnel-Private-Group-Id for VLAN ID, Calling-Station-Id for client MAC). Export current AP VLAN configuration. Run a packet capture on the wireless uplink trunk port with Wireshark filter 'vlan

&& http' to document any unencrypted sensitive traffic traversing wireless segments before applying new controls — this establishes a pre-remediation evidence baseline for any future breach notification analysis.

Step 3: Update threat model — add Layer 1/2 MitM via AirSnitch-class attacks (T1557, T1557.002, T1557.004, T1040) to your wireless threat register; treat shared physical wireless infrastructure as an untrusted medium regardless of encryption standard in use

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: correlating threat intelligence into detection capability and updating threat models to improve future adverse event recognition

Controls: NIST IR-4 (Incident Handling) — threat model update is a direct preparation input to the detection and analysis phase; without AirSnitch-class techniques in the threat register, SOC analysts will not recognize the attack pattern, NIST RA-3 (Risk Assessment) — formal risk assessment update required to reflect that WPA3-Enterprise's per-session encryption does not prevent Layer 2 MitM traffic interception or injection as demonstrated by AirSnitch, NIST SI-5 (Security Alerts, Advisories, and Directives) — ingest NDSS 2026 paper findings, CISA advisories, and vendor bulletins from Cisco, Ubiquiti, Netgear, and D-Link as formal threat intelligence inputs to the risk register, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update vuln management process to include protocol-design-class weaknesses (no CVE, no patch) as a risk category distinct from patchable software flaws

Compensating: Without a commercial threat intel platform: create a free MITRE ATT&CK Navigator layer (attack.mitre.org/resources/attack-navigator) annotating T1557 (Adversary-in-the-Middle), T1557.002 (ARP Cache Poisoning), T1557.004 (Wi-Fi Evil Twin AP — closest existing sub-technique), and T1040 (Network Sniffing) with AirSnitch context notes. Subscribe to the CISA Known Exploited Vulnerabilities (KEV) RSS feed and the NVD data feed filtered by keyword 'Wi-Fi' and 'wpa_supplicant'. Set a Google Alert for 'AirSnitch' and 'hostapd CVE' to track vendor patch releases. Document the threat register update as a dated artifact in your GRC system or a version-controlled markdown file.

Evidence: Before updating the threat model, document the current state: export your existing wireless threat register entries and note the absence of Layer 2 MitM without decryption as a recognized attack class. Preserve the NDSS 2026 paper citation (Schepers et al., NDSS 2026) and any vendor security advisories retrieved as PDFs with retrieval timestamps — these are your evidence artifacts demonstrating due diligence in threat intelligence consumption per NIST SI-5 (Security Alerts, Advisories, and Directives). If a prior wireless risk assessment exists, preserve that document before modification to show delta for audit purposes.

Step 4: Communicate findings — brief leadership that WPA3-Enterprise does not eliminate wireless MitM risk; frame the issue as an architectural gap, not a patch-and-done vulnerability; connect the risk to specific high-value environments (executive areas, R&D segments, financial systems on Wi-Fi)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned communication, reporting findings to leadership, and driving architectural improvements informed by threat analysis

Controls: NIST IR-6 (Incident Reporting) — while no active incident is confirmed, IR-6 requires communicating identified risks with potential incident impact to appropriate organizational levels; AirSnitch's viability against executive and financial Wi-Fi segments meets the threshold for leadership notification, NIST IR-8 (Incident Response Plan) — brief leadership as part of updating the IR plan to reflect that wireless MitM is now a credible pre-incident condition, not a theoretical risk, NIST RA-3 (Risk Assessment) — leadership briefing must include a risk statement that quantifies blast radius: AirSnitch enables MitM against any Wi-Fi client on affected APs (Netgear, D-Link, Ubiquiti, Cisco) regardless of WPA2 or WPA3-Enterprise encryption, affecting all client OSes in scope, CIS 7.2 (Establish and Maintain a Remediation Process) — frame the briefing around the documented remediation strategy: no patch available, architectural compensating controls (per-client VLAN, application-layer TLS, ZTNA) are the mitigation path

Compensating: Produce a one-page risk memo (not a slide deck) that states: (1) affected assets by location — executive conference room APs (vendor/model), R&D segment APs, financial system Wi-Fi uplinks; (2) attack scenario in plain language — an attacker on the same Wi-Fi network can intercept or inject traffic between clients without decrypting WPA3 by exploiting protocol-level client isolation bypass; (3) current compensating controls in place and gaps identified in Step 2; (4) recommended actions with effort/cost estimates. Use the NIST CSF 2.0 GOVERN

function framing to connect the architectural gap to organizational risk appetite. No specialized tools required.

Evidence: Attach to the leadership briefing: the AP inventory from Step 1 (timestamped), the VLAN/TLS gap findings from Step 2, and the threat register update from Step 3 as supporting evidence. Document the briefing date, attendees, and decisions made — this record satisfies NIST IR-6 (Incident Reporting) documentation requirements and provides a defensible audit trail if a wireless MitM incident occurs post-notification and regulatory inquiry follows.

Step 5: Monitor developments — track Unit 42, NDSS 2026 paper publication, and affected vendor advisories (Cisco, Ubiquiti, Netgear, D-Link) for firmware updates, protocol-level mitigations, or updated guidance from CISA; no patch currently addresses the root protocol design issue

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: continuous improvement through threat intelligence monitoring and updating detection/response capability as new information on a disclosed threat emerges

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formally assign ownership for monitoring Cisco PSIRT (tools.cisco.com/security/center), Ubiquiti Security Advisory RSS, Netgear security advisories, and D-Link security bulletins for AirSnitch-related firmware releases, NIST IR-5 (Incident Monitoring) — establish a monitoring cadence (recommend weekly) for AirSnitch-class detection signals on wireless segments: anomalous client-to-client traffic within the same SSID/VLAN that should be isolated, NIST CA-7 (Continuous Monitoring) — integrate AirSnitch-specific detection logic into continuous monitoring: look for unexpected ARP responses or ICMP redirects sourced from wireless client MAC addresses that should be isolation-enforced, CIS 7.3 (Perform Automated Operating System Patch Management) — extend patch management scope to AP firmware; configure automated firmware update checks on Ubiquiti UniFi Controller (Settings > System > Updates) and Cisco WLC auto-install staging, CIS 8.2 (Collect Audit Logs) — ensure AP association/disassociation logs and RADIUS accounting logs are being collected to a log aggregator outside the wireless segment so they cannot be tampered with if an AirSnitch-class attacker gains a position on the wireless network

Compensating: Without a SIEM: deploy Kismet (kismetwireless.net) in passive monitor mode on a dedicated interface to log all 802.11 management and data frames; configure Kismet alerts for unexpected BSS Transition frames and probe responses that could indicate rogue AP activity adjacent to AirSnitch exploitation. Write a weekly cron job that runs 'diff' against AP firmware version strings collected via SNMP sysDescr (snmpwalk) against a known-good baseline file — any change triggers email notification. Subscribe to CISA's free email alerts at cisa.gov/subscribe-updates-cisa and filter for 'Wi-Fi', 'wpa_supplicant', and 'hostapd' keywords. For Cisco-heavy environments, set up a free Cisco Security Advisory RSS feed subscription targeting the Cisco Wireless and IOS-XE advisory categories.

Evidence: Maintain a dated monitoring log documenting: each vendor advisory checked (URL, date, version reviewed), firmware versions deployed vs. available, and any Kismet or packet-capture anomalies observed on wireless segments (captured pcap files with 802.11 client-to-client traffic that bypasses expected isolation). If Kismet detects unexpected client-to-client frames on an isolation-enforced SSID, preserve the full pcap and Kismet alert log — these are your primary forensic evidence of a potential AirSnitch-class exploitation attempt and must be retained per NIST AU-11 (Audit Record Retention) timelines.

Detection Guidance

AirSnitch operates below the cryptographic layer, which makes signature-based detection at the application or transport layer ineffective. Detection requires visibility at the wireless and network layers.

Wireless layer: Deploy wireless intrusion detection/prevention system (WIDS/WIPS) capable of detecting rogue or unexpected 802.11 management frame patterns, unexpected client association sequences, and anomalous Layer 2 behavior such as duplicate MAC addresses or unexpected deauthentication frames. Commercial WIDS solutions and open-source tools (Kismet, Zeek with 802.11 support) can surface these patterns.

Network layer: Monitor for ARP anomalies on wireless segments, unexpected ARP replies, gratuitous ARPs from client MACs, and ARP table churn on access switches or wireless controllers are indicators consistent with

Layer 2 MitM positioning (T1557.002). Enable ARP inspection (Dynamic ARP Inspection on Cisco infrastructure) and log violations.

Traffic patterns: Look for unusual lateral traffic between wireless clients on the same SSID or VLAN, particularly clients that should not be communicating directly. Baseline normal client-to-client traffic volumes; deviations on wireless segments warrant investigation.

Endpoint telemetry: On managed endpoints, monitor for unexpected changes to ARP tables, default gateway MAC address changes, or certificate validation failures that may indicate traffic is being intercepted and re-presented.

Log sources to prioritize: Wireless controller logs (association events, deauth events, rogue AP alerts), DHCP server logs (unexpected lease requests from known MACs), network flow data on wireless uplinks, and endpoint security event logs for TLS certificate warnings or unexpected network path changes.

Hunting hypothesis: Search for wireless client pairs with traffic flows that do not terminate at the wireless controller or upstream gateway, any direct client-to-client flow on an enterprise SSID that enforces isolation is anomalous and should be investigated.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Unit 42 (Palo Alto Networks) and NDSS 2026 paper for published proof-of-concept tooling and indicators`	AirSnitch proof-of-concept tooling and attack framework details are expected to be documented in the full NDSS 2026 paper; Unit 42 technical coverage at https://unit42.paloaltonetworks.com/air-snitch-enterprise-wireless-attacks/ is the primary reference for any published indicators or tooling signatures	LOW

Framework Mappings

MITRE-ATTACK

- **T1556** — Modify Authentication Process
- **T1557** — Adversary-in-the-Middle
- **T1557.002** — ARP Cache Poisoning
- **T1200** — Hardware Additions
- **T1565** — Data Manipulation
- **T1557.004** — Evil Twin
- **T1040** — Network Sniffing
- **T1565.002** — Transmitted Data Manipulation
- **T1199** — Trusted Relationship

NIST-800-53R5

- **AC-6** — Least Privilege

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1556	Modify Authentication Process	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1557.002	ARP Cache Poisoning	Credential-Access
T1200	Hardware Additions	Initial-Access
T1565	Data Manipulation	Impact
T1557.004	Evil Twin	Credential-Access
T1040	Network Sniffing	Credential-Access
T1565.002	Transmitted Data Manipulation	Impact
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/air-snitch-enterprise-wireless-...	T3
	https://unit42.paloaltonetworks.com/air-snitch-enterprise-wireless-...	T3
	https://arstechnica.com/security/2026/02/new-airsnitch-attack-break...	T2
	https://hothardware.com/news/airsnitch-attack-can-intercept-encrypt...	T3
networking - WPA3-enterprise on Ubuntu	https://askubuntu.com/questions/1503195/wpa3-enterprise-on-ubuntu	T3

Generated 2026-04-23 06:38 UTC by TJS Security Command Center