



DOCUMENT INTEGRITY NOTICE: This document is subject to the Protocol Revision Policy (Section 8). Any revision must reproduce all sections in their complete, unabridged form. Abridgment, summarization, paraphrasing, or omission of any content constitutes a controlled document non-conformance.



AIRETOS Module Security Advisory — WLAN and Bluetooth Vulnerabilities, August and September 2026 IC Vendor Bulletins

OEM Security Advisory | DCN# 05A-SAOGEN-02 | Revision A | 2026-10-01

PUBLIC — for VOXMICRO customers and integrators



NOTICE

Accuracy and change

The information in this document has been carefully reviewed and is believed to be accurate. Nonetheless, this document is subject to change without notice, and VOXMICRO LTD (VOXMICRO) assumes no responsibility for any inaccuracies that may be contained in this document and makes no commitment to update or to keep current the contained information, or to notify a person or organization of any updates.

Proprietary information and reproduction

No part of this document may be reproduced, adapted or transmitted in any form or by any means, electronic or mechanical, for any purpose, except as expressly set forth in a written agreement signed by VOXMICRO.

Intellectual property

VOXMICRO or its affiliates may have patents or pending patent applications, trademarks, copyrights, mask work rights or other intellectual property rights that apply to the ideas, material and information expressed herein. No license to such rights is provided except as expressly set forth in a written agreement signed by VOXMICRO. VOXMICRO does not represent that products described herein are free from patent infringement or from any other third party right.

Copyright

© 2026 VOXMICRO LTD. All rights reserved.

Warranty and liability

VOXMICRO LTD. MAKES NO WARRANTIES OF ANY KIND WITH REGARD TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT SHALL VOXMICRO LTD. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATORY OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, VOXMICRO LTD. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA TRANSMITTED OR OTHERWISE USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE OR DATA.

Implied warranties

VOXMICRO LTD. SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AS THEY MIGHT OTHERWISE APPLY TO THIS DOCUMENT AND TO THE IDEAS, MATERIAL AND INFORMATION EXPRESSED HEREIN.

Third-party trademarks

Qualcomm and QCA are trademarks or registered trademarks of Qualcomm Incorporated. The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. Wi-Fi® and Wi-Fi 6E® are registered trademarks of Wi-Fi Alliance. PCI Express® and PCIe® are registered trademarks of PCI-SIG. All other trademarks, trade names and product names referenced herein are the property of their respective owners.

Product terms

Products described in VOXMICRO documents are sold exclusively under the VOXMICRO Terms & Conditions of Sale and the VOXMICRO Warranty Policy, provided with VOXMICRO's quotation and order acknowledgment. No warranty, liability or other transaction terms are granted or accepted through this document.

NOTICE — Rev. A (2026-10-01)

Revision History

Rev	Date	Description
A	2026-10-01	Initial release (document finalised 2026-10-01; issued following direct customer notification per VDP §8.2 — see publication date on the advisories page). Covers the August 2026 (published 2026-08-03) and September 2026 (published 2026-09-07) IC vendor bulletins in one advisory. Seven items applicable to AIRETOS classes; CVE-2026-25289 (Critical) reachability verification in progress (§3); three items under assessment (§7.1). Host-stack minimum versions added (§5).

Table of Contents

1. Summary	5
2. Affected Products	5
3. Vulnerability Details	6
4. Corrective Action — Firmware / BSP Updates	7
5. Interim Mitigations and Host-Stack Guidance	7
6. Risk Assessment Guidance for OEM Integrations	8
7. Not Affected — Items Listing AIRETOS Chipsets in Non-Applicable Components	8
7.1 Under assessment	9
8. References	9

Advisory ID: 05A-SAOGEN-02 · **Revision:** A · **Date:** 2026-10-01 **Related:** 05A-SAOGEN-01 Rev B (April–July 2026 IC vendor bulletins) **Contact:** vdp+security@voxmicro.com

1. Summary

VOXMICRO monitors the IC vendor's monthly public security bulletins as part of its vulnerability management program (Vulnerability Disclosure Policy 05V-SVOGEN-01). The **August 2026 bulletin (published 2026-08-03, thirteen CVEs)** and the **September 2026 bulletin (published 2026-09-07, seventeen CVEs)** have been reviewed in full against the complete AIRETOS chipset portfolio. This advisory covers both.

Seven items are applicable to AIRETOS module firmware, host drivers or BSP packages. A further sixteen list an AIRETOS chipset but concern host-platform functions that AIRETOS wireless modules do not implement (§7).

Key points for OEM customers:

- **No vulnerability in either bulletin is reported as exploited in the wild.** Neither bulletin carries an exploitation statement, and no AIRETOS-applicable item appears in national known-exploited-vulnerability catalogues as at the date of this advisory.
- **One item is rated Critical.** CVE-2026-25289 (CVSS 9.6) is a stack-based buffer overflow in WLAN firmware, triggerable over the air without authentication, in the NAN (Wi-Fi Aware) service discovery path. It lists the **E92 and C27** chipsets. Its practical reachability in AIRETOS firmware is under verification — see §3.
- **E20 is affected by one High item** — CVE-2026-25275 (7.5), a transient denial-of-service in WLAN firmware when parsing malformed FILS authentication frames. Availability impact only; self-recovering; no data exposure or code execution. Also one Medium Windows-host item (CVE-2026-24076).
- **E92 and C27 have not reached market introduction.** Corrective firmware forms part of their production launch baseline rather than a field update. Units in circulation are engineering samples and evaluation kits held under non-disclosure agreement.
- **Open-source host components:** five upstream hostapd / wpa_supplicant advisories published June–August 2026 and a set of Linux wireless kernel fixes affect OEM host software used with AIRETOS modules. Minimum versions are given in §5.

2. Affected Products

Applicability determined against the affected-chipset lists in the IC vendor's August and September 2026 bulletins, cross-referenced against the chipsets used in each AIRETOS class. "Affected" means the module's chipset is listed by the IC vendor; operational applicability may be narrower (§3).

CVE	Bulletin	Severity (vendor CVSS v3.1)	E20	E92	C27
CVE-2026-25289	Aug	Critical 9.6	Not affected	Affected	Affected
CVE-2026-25275	Sep	High 7.5	Affected	Affected	Affected
CVE-2026-25288	Aug	High 7.4	Not affected	Not affected	Affected
CVE-2026-25294	Sep	High 7.4	Not affected	Not affected	Affected
CVE-2026-24081	Sep	High 7.4	Not affected	Listed ²	Affected
CVE-2026-24077	Aug	Medium 6.5	Not affected	Affected	Affected ¹
CVE-2026-24076	Aug	Medium 6.7	Affected	Not affected	Affected

¹ Via the companion IC listing; the C27 WLAN SoC platform is not listed for CVE-2026-24077. ² CVE-2026-24081 is a Bluetooth controller firmware issue. The E92 chipset is listed, but E92 modules do not implement a Bluetooth controller; confirmation of non-applicability is in progress.

All form-factor variants within a class (LGA CoB and on-carrier M.2 / mPCIe) share the same chipset and firmware and therefore the same applicability.

Legacy classes. E95 chipsets appear on no item in either bulletin. The E98 class is under assessment for CVE-2026-25275 (§7.1). E61/E63 are legacy build-to-order classes; their chipsets appear only on CVE-2026-25275 and CVE-2026-24076, and customers of those classes should contact vdp+security@voxmico.com for a position.

Production status. E20 is in series production and deployed in customer products. E92 and C27 have not reached market introduction; see §4.

3. Vulnerability Details

CVE	Subsystem	Nature	Access Vector	Impact
CVE-2026-25289	WLAN firmware — NAN (Wi-Fi Aware) Service Discovery Frame parsing	Stack-based buffer overflow when processing Device Capability Extended attributes with invalid length values	Adjacent RF (AV:A), unauthenticated, no user interaction, scope-changed	Confidentiality / Integrity / Availability (C:H/I:H/A:H)
CVE-2026-25275	WLAN firmware — authentication frame parsing (FILS information element)	Buffer over-read when processing authentication frames with invalid FILS IE header lengths	Network (AV:N as scored by vendor; practically adjacent RF), unauthenticated, pre-association	Transient DoS (availability only, A:H)
CVE-2026-25288	WLAN firmware — Target Wake Time (TWT) channel usage	Buffer over-read on a short TWT channel-usage response frame	Adjacent RF, unauthenticated, scope-changed	Transient DoS
CVE-2026-25294	WLAN firmware — frame parsing during channel usage	Buffer over-read while parsing a frame during channel usage	Adjacent RF, unauthenticated, scope-changed	Transient DoS
CVE-2026-24081	Bluetooth controller firmware — adaptive frequency hopping	Buffer over-read when processing a channel map with insufficient used channels while AFH is fully enabled	Adjacent RF, unauthenticated, scope-changed	Transient DoS
CVE-2026-24077	WLAN host driver — channel switch information	Integer underflow on improperly formatted channel-switch length fields	Adjacent RF, unauthenticated	Information disclosure (C:H)
CVE-2026-24076	Bluetooth host (Windows) — registry value handling	Buffer copy without size validation on registry values of incorrect type	Local, high privileges required	Memory corruption (C:H/I:H/A:H)

Exploitation status: no exploitation statement in either bulletin; no AIRETOS-applicable item in national known-exploited-vulnerability catalogues as at the date of this advisory.

CVE-2026-25289 — reachability under verification. *Established:* the IC vendor lists the E92 and C27 chipsets and rates the issue Critical. The vulnerable code path parses NAN (Wi-Fi Aware) Service Discovery Frames — frames any transmitter in radio range can emit, processed before any security association exists. *Not yet established:* whether the NAN feature is present and enabled in the firmware images VOXMICO ships for E92 and C27. NAN is an optional Wi-Fi feature and is frequently excluded from embedded firmware builds; if it is not built in, the vulnerable parser is not reachable in an AIRETOS configuration. This advisory will be revised when verification concludes. §5 item 1 gives the configuration-level measure that removes exposure regardless of outcome.

CVE-2026-25275 — the E20 item. The affected parser handles the FILS (Fast Initial Link Setup, IEEE 802.11ai) information element in authentication frames. FILS is an optional fast-roaming feature; a module not configured for FILS still receives authentication frames, so the parser may be exercised regardless of configuration. The consequence is a firmware reset with autonomous recovery — a brief loss of wireless connectivity — not data exposure or code execution. Same vulnerability family as CVE-2026-21367 (April–July advisory).

CVE-2026-24076. Windows Bluetooth host stack, not module firmware; requires an already-privileged local actor; does not apply to Linux BSP packages.

4. Corrective Action — Firmware / BSP Updates

Item	Class(es)	Corrective action	Availability
CVE-2026-25275	E20 (Linux, Windows)	Corrective WLAN firmware incorporated in the next E20 CLD maintenance release	In preparation — version and date to be announced in a revision of this advisory
CVE-2026-24077	E92, C27 (Linux)	Fix available in the open-source WLAN host driver; integration does not depend on a proprietary firmware drop	In preparation
CVE-2026-25289, CVE-2026-25288, CVE-2026-25294, CVE-2026-25275	E92, C27 (module firmware)	Corrective firmware incorporated in the production launch baseline	Pre-production classes — see note
CVE-2026-24081	C27 (Bluetooth controller firmware)	Corrective firmware incorporated in the production launch baseline	Pre-production class
CVE-2026-24076	E20, C27 (Windows)	Included in the Windows driver update train	To be announced

E92 / C27 — pre-production classes. Neither class has reached market introduction. The corrective firmware is a **gating item for production launch**: these classes will not reach market introduction without the applicable fixes incorporated into, or formally assessed as not applicable to, the launch BSP baseline. Holders of engineering samples and evaluation kits should apply §5 during bring-up and will receive the corrective baseline through their existing NDA engineering channel.

E20. One firmware action arises (CVE-2026-25275), delivered through the normal maintenance train; no emergency action is required, since the impact is a transient, self-recovering availability loss. Deploy the corrective release at the next maintenance window. The Windows Bluetooth item follows the Windows driver update train.

Upstream dependency. Per VDP §5.5, VOXMICRO's remediation timelines begin on receipt of the corresponding upstream patch. Where availability is shown as pending, the dependency is upstream availability and integration validation.

5. Interim Mitigations and Host-Stack Guidance

Module-level (configuration):

- **Disable NAN / Wi-Fi Aware where the application does not require it** (CVE-2026-25289). Decisive rather than mitigating: if the NAN service discovery path is not enabled, the vulnerable parser is not exercised. Most embedded and industrial deployments do not use Wi-Fi Aware.
- **Disable FILS authentication where not required** (CVE-2026-25275) — `file_discovery/FILS` AKMs off in `hostapd`; no FILS key management in `wpa_supplicant` network blocks. This reduces but may not eliminate exposure (see §3); the firmware update is the remedy.
- **TWT policy on power-sensitive C27 deployments** (CVE-2026-25288, CVE-2026-25294). Where Target Wake Time is not required, disabling it removes exposure; impact is availability only.
- **Enable 802.11w Protected Management Frames** (`ieee80211w=2`) on all SSIDs where the client population allows. Raises the bar for spoofed management-frame injection generally; does not protect the pre-association frame classes in CVE-2026-25289/25275.
- **Restrict local privilege on Windows hosts** (CVE-2026-24076).
- **RF-environment hardening** for high-assurance deployments: WIDS monitoring for malformed management frames and clustered client disconnects.

Host software (OEM-maintained; VDP §5.5):

- **hostapd / wpa_supplicant minimum versions.** Five upstream advisories published 2026-06-30 to 2026-08-17 affect the Wi-Fi 7 multi-link association path (hostapd, unauthenticated DoS — CVE-2026-58374, covered in 05A-SAOGEN-01 Rev B), PMKSA cache network-context validation (wpa_supplicant — an authentication-step bypass by a rogue AP holding any valid credential), SAE H2E commit parsing (wpa_supplicant, DoS), secure-mesh AMPE bounds checking (wpa_supplicant, post-authentication heap overflow) and RADIUS Message-Authenticator length validation (hostapd, DoS in Enterprise/RADIUS configurations). **Minimum: hostapd 2.12.1 and wpa_supplicant 2.12**, or the corresponding upstream commits backported. Enterprise (RADIUS) AP builds and WPA3-SAE station builds are the exposed profiles.
- **Linux kernel wireless stack.** Fixes published August 2026 in the generic 802.11 stack (mac80211, cfg80211 — extension-frame validation, block-ack session teardown, multi-link element validation) and in the AIRETOS-relevant drivers (ath12k for E92/C27; ath11k for E20) are in all maintained stable branches. Use a current stable kernel on your branch; the 6.19 and 7.0 series are end of life and must move to 7.1.x or later. Distribution kernels commonly backport without rebasing — the distribution changelog, not the version string, is the authority.

6. Risk Assessment Guidance for OEM Integrations

- **CVE-2026-25289** warrants attention for its access profile: adjacent RF, no authentication, no user interaction, pre-association, scope-changed, full impact. Where NAN is enabled in an environment where an attacker could plausibly be within radio range, treat it as the priority. Where NAN is disabled or not built in, exposure does not arise.
- **CVE-2026-25275 (E20 and all active classes)** is a transient, self-recovering loss of wireless connectivity triggered by a malformed frame from radio range. Availability-critical deployments (industrial control, medical telemetry) should take the corrective release promptly; others in the normal maintenance train.
- **CVE-2026-25288 / 25294 / 24081** are the same class of transient DoS, confined to C27 (pre-production). Launch-baseline items.
- **CVE-2026-24077** discloses memory contents to an unauthenticated party in radio range; Medium score but confidentiality-class impact.
- **CVE-2026-24076** is routine maintenance (local, privileged, Windows only).
- **No item in either bulletin requires emergency action for any deployed AIRETOS product.**

7. Not Affected — Items Listing AIRETOS Chipsets in Non-Applicable Components

Both bulletins list AIRETOS chipsets on further CVEs concerning host-platform functions that AIRETOS wireless modules do not implement. They are set out explicitly because a reader cross-referencing the published bulletins against AIRETOS chipset data will encounter them.

CVE	Bulletin	Component	Why not applicable to AIRETOS
CVE-2026-24084 (High)	Aug	Multi-mode call processor	3GPP cellular UE security-capability negotiation. No cellular function in any AIRETOS module.
CVE-2026-24078 (Medium)	Aug	Cellular data modem — emergency-call signalling	Automotive NG-eCall. Not present in any AIRETOS BSP.
CVE-2026-25292 (High)	Aug	Automotive Linux OS — bootloader command handler	Requires physical access; host-platform bootloader component. AIRETOS modules ship no such bootloader.
CVE-2026-24080 (High)	Aug	Biometrics	No biometric function in any AIRETOS product.
CVE-2026-6726, CVE-2026-6727 (High)	Aug/Sep	Windows Compute — TPM 2.0 reference implementation	Platform firmware TPM / attestation on compute SoCs. AIRETOS modules carry no TPM and no attestation function.

CVE	Bulletin	Component	Why not applicable to AIRETOS
CVE-2025-59607 (High)	Sep	Windows Compute	Host compute-platform driver.
CVE-2026-24073, CVE-2026-24074 (High)	Sep	Video	Video codec subsystem of host SoCs; no video function in a WLAN/BT module.
CVE-2026-25261 (Medium)	Sep	Camera	No camera function.
CVE-2026-24075 (High)	Sep	Inter-processor communication	Host-SoC IPC driver.
CVE-2026-25278 (High)	Sep	Automotive software platform (QNX)	Automotive host OS; not shipped with AIRETOS modules.
CVE-2026-25280 (High)	Sep	DSP service	Host DSP subsystem.
CVE-2026-25281 – 25284, CVE-2026-25290 (High)	Sep	Out-of-band management (compute platforms)	Compute-platform management controller; no such function in a WLAN/BT module.

The listings arise from the vendor's platform-wide enumeration pattern, in which a combination connectivity chip appears on affected-product lists for host platforms that incorporate it.

7.1 Under assessment

- **CVE-2026-24079** (High 8.1, cellular data modem — missing authentication on registration requests; Aug) lists the E92 and C27 chipsets. The affected component performs cellular modem registration, which AIRETOS modules do not implement. A formal assessment is being completed rather than closing on reasoning alone because of its score and access vector.
- **CVE-2026-25275 — E98 class.** The vendor's affected list includes parts in the family used by the E98 class; applicability to shipped E98 modules is being confirmed.
- **CVE-2026-24081 — E92.** See §2 note ².

This advisory will be revised if any assessment changes the position.

8. References

- IC vendor public security bulletins, August 2026 (published 2026-08-03) and September 2026 (published 2026-09-07) — docs.qualcomm.com/product/publicresources/securitybulletin
- CVE records (cve.org): CVE-2026-25289, CVE-2026-25275, CVE-2026-25288, CVE-2026-25294, CVE-2026-24081, CVE-2026-24077, CVE-2026-24076, CVE-2026-24079
- hostapd / wpa_supplicant security advisories 2026-1 to 2026-5 — w1.fi/security/
- VOXMICRO advisory 05A-SAOGEN-01 Rev B — WLAN vulnerabilities, April–July 2026 IC vendor bulletins
- VOXMICRO Vulnerability Disclosure Policy: [05V-SVOGEN-01 Rev A](<https://www.voxmicro.com/security>)
- Security contact: vdp+security@voxmicro.com