AIRETOS Module Security Advisory

WLAN Vulnerabilities Disclosed in the April–July 2026 IC Vendor Security Bulletins

OEM Security Advisory | DCN# 05A-SAOGEN-01 | Revision B | August 11, 2026
Supersedes Revision A (2026-07-14) · vdp+security@voxmicro.com

PUBLIC — for VOXMICRO customers and integrators

NOTICE

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. VOXMICRO reserves the right to make changes, at any time, in order to improve reliability, function or design and to attempt to supply the best product possible. VOXMICRO does not represent that products described herein are free from patent infringement or from any other third party right.

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. 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 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. 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.

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.

Third-Party Trademarks: Wi-Fi® is a trademark of the Wi-Fi Alliance. Bluetooth® is a trademark of Bluetooth SIG, Inc. Qualcomm® is a trademark of Qualcomm Incorporated. All other trademarks, trade names and product names referenced herein are the property of their respective owners.

NOTICE — Rev. B (2026-07-25)

Revision History

Rev	Date	Change summary	Author	Approved By
A	2026-07-14	Initial public release. E20 v1.3 availability confirmed (released to OEM customers 2026-07-09).	Product Security (VDP)	Management / Legal
B	2026-08-11	Scope correction and status update. §5: added item 4 covering upstream hostapd CVE-2026-58374 (published 2026-06-30, within the April–July window; omitted from Rev A), placed in Interim Mitigations as a host software item rather than an IC vendor bulletin item. §6: corresponding risk-assessment note. §1/§2: production-status statement — E92 and C27 are pre-production; corrective firmware forms part of the launch baseline rather than a field update. §4: E92/C27 rows restated on that basis; upstream-dependency statement per VDP §5.5; new §4.1 open-items table. §2/§3: explicit status on the two assessments left open at Rev A. §8: hostapd reference added.	Product Security (VDP)	Management / Legal

Table of Contents

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 April, May, June, and July 2026 bulletins have each been reviewed in full against the complete AIRETOS chipset portfolio, using the vendor's canonical per-CVE affected-product records.

- The **June 2026 bulletin contains no items affecting any AIRETOS product** (its flagged vulnerabilities are confined to mobile application processors). No customer action arises from June.
- The **April and May 2026 bulletins** disclose four WLAN-area vulnerabilities affecting AIRETOS classes (§2–§3).
- The **July 2026 bulletin** adds one applicable item, CVE-2026-25268 (WLAN host driver, local vector); all eleven July items carry a local attack vector — none are triggerable over the air.

Key points for OEM customers:

- **No vulnerability in this set is known to be exploited in the wild.**
- Three of the four April/May items are **transient denial-of-service** issues (wireless connectivity disruption, self-recovering); one (CVE-2025-47392) is a memory-corruption issue in GNSS assistance-data decoding with an adjacent-network vector.
- **E92 and C27 classes are the primary focus.** E20 is formally affected by one Medium-severity item only.
- **E92 and C27 are pre-production classes** and have not reached market introduction. Corrective firmware for these classes will be incorporated into the launch BSP baseline rather than issued as a field update — see §4.
- Corrective firmware is delivered through VOXMICRO BSP releases (§4). Interim configuration mitigations are available for the roaming-related item (§5).
- The widely publicized "unpatchable BootROM" vulnerability (CVE-2026-25262) does **not** affect any AIRETOS module — see §7.

Added in Revision B: §5 now includes guidance on **CVE-2026-58374**, an upstream `hostapd` vulnerability published 2026-06-30 that falls within this advisory's reporting window. It is not an IC vendor bulletin item and therefore does not appear in §2 or §3, but it is relevant to any AIRETOS deployment operating in access-point mode with Wi-Fi 7 Multi-Link Operation enabled. See §5 item 4.

Scope note: the August 2026 IC vendor bulletin falls outside this advisory's window and will be addressed in a separate advisory in this series.

2. Affected Products

Applicability verified against the IC vendor's canonical CVE records (per-chipset affected lists), 2026-07-07. "Affected" means the module's chipset is listed by the IC vendor; operational applicability may be narrower (see per-CVE notes).

CVE	Severity (vendor CVSS v3.1)	E20 class (all variants)	E92 class (all variants)	C27 class (all variants)
CVE-2025-47392	High 8.8	Not affected	**Affected**	**Affected** [1]

CVE	Severity (vendor CVSS v3.1)	E20 class (all variants)	E92 class (all variants)	C27 class (all variants)
CVE-2026-21367	High 7.6	Not affected	**Affected**	**Affected**
CVE-2025-47401	Medium 6.5	**Affected**	**Affected**	**Affected**
CVE-2025-47403	Medium 6.5	Not affected	**Affected**	**Affected**
CVE-2026-25268 (July)	High 8.8 (local)	Not affected	**Affected**	**Affected** [1]

[1] Via the Bluetooth companion IC listing; the C27 WLAN SoC platform is not listed for CVE-2025-47392 or CVE-2026-25268.

Two further July items (CVE-2026-25271, DSP Service; CVE-2026-21379, Windows Compute — both High, local-only) list the C27 SoC platform but concern host-compute components; VOXMICRO engineering is assessing whether the affected code is present in any C27 driver package.

> **Revision B status (2026-08-11):** this assessment **remains open**. Neither item has been confirmed applicable to any C27 driver package, and neither has been excluded. The advisory will be revised when the assessment concludes. Customers requiring a definitive position before that point should contact vdp+security@voxmicro.com.

Production status of the affected classes (added in Revision B). E20 is in series production and deployed in customer products. **E92 and C27 have not reached market introduction**; units in circulation are engineering samples and evaluation kits held under non-disclosure agreement. For those two classes the corrective firmware identified in §4 will form part of the production launch baseline, and no field-update campaign arises.

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.

3. Vulnerability Details

CVE	Subsystem	Nature	Access Vector	Impact
CVE-2025-47392	GNSS assistance-data decode	Integer overflow → memory corruption when decoding corrupted satellite data files with invalid signature offsets	Adjacent network (AV:A), no privileges, no user interaction	Confidentiality/Integrity/ Availability (C:H/I:H/A:H)
CVE-2026-21367	WLAN firmware — FILS Discovery frame parsing	Buffer over-read on nonstandard FILS Discovery frames with out-of-range action sizes during initial scans	Over-the-air, during scan	Transient DoS (wireless subsystem recovery)
CVE-2025-47401	WLAN HAL — channel configuration	Buffer over-read while processing target power rate tables during channel configuration	Adjacent (AV:A)	Transient DoS

CVE	Subsystem	Nature	Access Vector	Impact
CVE-2025-47403	WLAN firmware — 802.11r Fast Transition	Buffer over-read on malformed FT response frames during roaming; processed pre-authentication, no user interaction	Adjacent RF, unauthenticated	Transient DoS
CVE-2026-25268	WLAN host driver — dynamic channel switching	Stack-based buffer overflow when processing invalid HT40 channel layouts during dynamic channel switching	**Local** (AV:L, host-side; not triggerable over RF)	Memory corruption; potential host privilege escalation (C:H/I:H/A:H, scope-changed)

Exploitation status: no public proof-of-concept and no in-the-wild exploitation reported for any of these items as of the publication date of this revision.

Note on CVE-2025-47392: the vulnerable code path concerns GNSS assistance-data processing. AIRETOS modules do not implement standalone GNSS reception; VOXMICRO engineering is verifying whether the affected code is present in module firmware images.

> **Revision B status (2026-08-11):** this verification **remains open**. Until it concludes, the risk guidance in §6 stands — treat E92/C27 in adversarial-RF environments as the priority population. The advisory will be revised when the verification concludes.

4. Corrective Action — Firmware / BSP Updates

Fixes for the items above are incorporated in the IC vendor's April/May 2026 patch sets and are delivered to OEM customers through VOXMICRO BSP releases:

Class	Platform	Fixed BSP / firmware version	Availability
E20	Linux	**E20 CLD Linux FW v1.3** (maintenance release; supersedes v1.2)	**Available** — released to OEM customers 2026-07-09
E92	Linux	To be incorporated in the production launch baseline	Pre-production class — see note below
C27	Linux	To be incorporated in the production launch baseline	Pre-production class — see note below
E20 / C27	Windows	Corrective driver package in preparation — version to be announced [2]	To be announced

[2] A separate Medium/local-only Windows WLAN host-driver item (CVE-2026-25266, CVSS 5.5, requires local privileged access) applies to the C27-class Windows driver package; it is included in the same Windows driver update train.

E20 note: the previously shipping E20 Linux package (v1.2) was baselined before the IC vendor's May 2026 patch set and does **not** contain the CVE-2025-47401 fix. E20 exposure is limited to this single Medium transient-DoS item; the fix is delivered in the normal maintenance-release train as **v1.3, released to OEM customers 2026-07-09**. No emergency action is required — deploy v1.3 at the next maintenance window.

E92 / C27 note (added in Revision B). These classes are pre-production (§2). Rather than a dated field release, the corrective firmware is a gating item for their production launch: the 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 the interim measures in §5 during bring-up and will receive the corrective baseline through their existing NDA engineering channel.

Upstream dependency. Per VDP §5.5, VOXMICRO's remediation timelines begin on receipt of the corresponding upstream patch from the IC vendor. Where a corrective firmware release is shown above as pending, the dependency is upstream availability and integration validation, not a VOXMICRO scheduling decision. VOXMICRO will state the specific fixed versions in a subsequent revision of this advisory as they are confirmed.

4.1 Open items and next update

Item	Section	Status at 2026-08-11
CVE-2026-25271 / CVE-2026-21379 applicability to C27 driver packages	§2	Open — assessment in progress
CVE-2025-47392 GNSS code-path presence in module firmware images	§3	Open — verification in progress
E92 / C27 Linux corrective versions	§4	Pending upstream patch receipt and launch-baseline integration
E20 / C27 Windows driver package version	§4	Pending release of the Windows driver update train

VOXMICRO will issue a further revision of this advisory when these items conclude. Customers requiring a position on any of them before that point should contact vdp+security@voxmicro.com.

5. Interim Mitigations (configuration-level)

These do not replace the firmware update but reduce the practically exploitable surface:

1. **Enable 802.11w Protected Management Frames (PMF)** on all SSIDs (`ieee80211w=2` in hostapd; require PMF where the client population allows). PMF raises the bar for spoofed management-frame injection generally. Note: FILS Discovery frames (CVE-2026-21367) are broadcast pre-association frames and are not protected by PMF; the firmware update is the effective remedy for that item.

2. **Review 802.11r Fast Transition policy** (CVE-2025-47403): the vulnerable path parses FT *response* frames in the station/roaming role. Deployments where the AIRETOS module operates as SoftAP only (including multi-SSID SAP configurations) do not exercise this path. For station-role deployments that roam, consider disabling FT (`wpa_supplicant`/infrastructure-side) on networks serving unpatched devices, where roaming performance requirements permit.
3. **Host stack currency:** for Wi-Fi 7 / MLO-capable designs (C27, E92), ensure host kernels include the fix for CVE-2026-46125 (mac80211 MLO station cleanup use-after-free, published 2026-05-28); restrict debugfs access on production images.
4. **Access-point software currency — `hostapd` CVE-2026-58374 (added in Revision B).** An upstream vulnerability published 2026-06-30 affects `hostapd` versions up to and including 2.11 when built with `CONFIG_IEEE80211BE` for AP-mode Wi-Fi 7 (802.11be) Multi-Link Operation. A missing bounds check in MLO association-request processing allows an unauthenticated attacker within wireless range to send a crafted management frame containing a malformed Multi-Link Element or Per-STA Profile subelement, causing an out-of-bounds write during association processing — before the four-way handshake. The confirmed practical impact is denial of service through `hostapd` process termination (CVSS 3.1 base score 7.1, `AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H`).

   This is a **host software** issue, not an AIRETOS module firmware defect. `hostapd`, and the decision to enable MLO in access-point mode, reside on the OEM host platform and outside VOXMICRO's shipped deliverables. VOXMICRO's guidance is therefore:

   - Where an AIRETOS Wi-Fi 7 class (E92, C27) is operated in **AP or SoftAP mode with MLO enabled**, ensure the host build uses **`hostapd` v2.12 or later**, or carries the upstream 2026-1 fix set.
   - Where moving to v2.12 is not immediately practical, disable MLO in AP mode, or build `hostapd` without `CONFIG_IEEE80211BE`, until the update can be applied.
   - **E20 is Wi-Fi 6E** and does not implement 802.11be; the vulnerable MLO association path is not reached on E20 designs. Integrators running E20 in SoftAP configurations may nonetheless wish to confirm their `hostapd` version as part of routine host maintenance.
5. **RF-environment hardening** for high-assurance deployments: WIDS monitoring for malformed management frames and clustered client disconnects can detect attempted exploitation of the DoS items.

6. Risk Assessment Guidance for OEM Integrations

- The three WLAN DoS items cause **temporary loss of wireless connectivity** with autonomous subsystem recovery; they do not compromise data confidentiality or integrity and do not provide code execution.
- Systems with availability-critical wireless links (e.g., safety-adjacent telemetry, real-time control) should prioritize the firmware update; repeated triggering could produce sustained denial of service while an attacker remains in RF range.
- CVE-2025-47392 carries a higher theoretical impact (memory corruption); pending the §3 engineering verification, treat E92/C27 deployments in adversarial-RF environments as the priority population.
- **CVE-2026-58374 (§5 item 4)** differs from the items in §2 in one respect worth noting for risk assessment: it is triggerable over the air by an unauthenticated party in radio range, against the access-point role, before any security association is established. Its impact is confined to availability.

Deployments running AIRETOS Wi-Fi 7 modules as access points with MLO enabled, on `hostapd` builds older than v2.12, should treat the host software update as the priority action.

7. Not Affected — BootROM / EDL Vulnerability (CVE-2026-25262)

The IC vendor's May 2026 bulletin includes a widely publicized, unpatchable BootROM vulnerability (CVE-2026-25262) exploitable via Emergency Download Mode with physical USB access. **No AIRETOS module is affected:** the vulnerability is confined to specific cellular modem and mobile application-processor chip series, none of which are used in any AIRETOS product. No customer action is required.

8. References

- IC vendor public security bulletins: April, May, June, July 2026 (docs.qualcomm.com/product/publicresources/securitybulletin)
- CVE records: CVE-2025-47392, CVE-2026-21367, CVE-2025-47401, CVE-2025-47403, CVE-2026-25268 (cve.org)
- CVE-2026-58374 and the upstream `hostapd` 2026-1 fix set (w1.fi/security/2026-1/)
- VOXMICRO Vulnerability Disclosure Policy: 05V-SVOGEN-01 Rev A
- Security contact: vdp+security@voxmicro.com

9. Revision History

Rev	Date	Description
DRAFT A	2026-07-07	Initial working draft covering April/May 2026 bulletin items.
DRAFT B	2026-07-07	Added July 2026 bulletin review: CVE-2026-25268 (WLAN host, local, 8.8) added to scope; June/July reviewed-bulletins statement added to §1; two July C27 items noted as under assessment (§2).
DRAFT C	2026-07-07	E20 Linux row (§4) completed per engineering verification: v1.2 baseline confirmed to predate the May 2026 patch set (fix not included); corrective release identified as E20 CLD Linux FW v1.3 (maintenance train), availability TBA.
A	2026-07-14	Initial public release. E20 v1.3 availability confirmed (released to OEM customers 2026-07-09).

Rev	Date	Description
B	2026-08-11	Scope correction and status update. §5: added item 4 covering upstream `hostapd` CVE-2026-58374 (published 2026-06-30, within this advisory's April–July window; omitted from Rev A) — placed in Interim Mitigations rather than §2/§3 because it is a host software item, not an IC vendor bulletin item. §6: added corresponding risk-assessment note. §1, §2: added production-status statement — E92 and C27 are pre-production classes; corrective firmware forms part of the launch baseline rather than a field update. §4: E92/C27 rows restated on that basis; upstream-dependency statement added per VDP §5.5; new §4.1 open-items table with commitment to a further revision. §2, §3: explicit status statements on the two assessments left open at Rev A. §8: added `hostapd` reference.

This advisory is provided for the information of VOXMICRO customers and integrators. It will be revised if applicability, corrective releases, or guidance change; revisions are announced via the Security Advisories RSS feed, linked from www.voxmicro.com/security/advisories.