AIRETOS Module Security Advisory — WLAN Vulnerabilities, April–July 2026 IC Vendor Bulletins

Security Advisory | DCN# 05A-SAOGEN-01 | Revision A | July 14, 2026

PUBLIC — Official Circulation

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.

Third-Party Trademarks

Wi-Fi® is a registered trademark of the Wi-Fi Alliance.
Bluetooth® is a registered trademark of Bluetooth SIG, Inc.
Qualcomm® is a registered trademark of Qualcomm Incorporated.
Windows® is a registered trademark of Microsoft Corporation.
Linux® is a registered trademark of Linus Torvalds.
All other trademarks, trade names, and product names referenced herein are the property of their respective owners.

Revision History

Rev	Date	Change summary	Author (role/team)	Approved By (role)	Evidence ID
A	2026-07-14	Initial public release.	VOXMICRO Product Security (VDP)	Management / Legal	05A-SAOGEN-01

Table of Contents

Advisory ID: 05A-SAOGEN-01 · **Revision:** A · **Published:** 2026-07-14 · **Contact:** vdp+security@voxmicro.com · **Policy:** 05V-SVOGEN-01 Rev A (www.voxmicro.com/security)

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.
- 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.

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-2026-21367	High 7.6	Not affected	**Affected**	**Affected**
CVE-2025-47401	Medium 6.5	**Affected**	**Affected**	**Affected**

CVE	Severity (vendor CVSS v3.1)	E20 class (all variants)	E92 class (all variants)	C27 class (all variants)
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 and CVE-2026-21379 — 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. This advisory will be revised if either is confirmed applicable.

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-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.

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. This advisory will be revised if the assessment changes.

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	Corrective BSP release in preparation — version TBC	To be announced
C27	Linux	Corrective BSP release in preparation — version TBC	To be announced
E20 / C27	Windows	Corrective driver package in preparation — version TBC [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 currently 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.

OEM customers should plan to move to the fixed BSP versions at their next maintenance window. Until then, the interim measures in §5 reduce exposure for the over-the-air items. This advisory will be revised as corrective-release versions and availability dates are announced.

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. **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.

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)
- VOXMICRO Vulnerability Disclosure Policy: 05V-SVOGEN-01 Rev A
- Security contact: vdp+security@voxmicro.com

9. Revision History

Rev	Date	Description
A	2026-07-14	Initial public release.

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.