



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.



Vulnerability Disclosure Policy

Compliance Statement | DCN# 05V-SVOGEN-01 | Revision A | March 16, 2026

Classification: Official — Public Distribution



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.

© 2006–2026 VOXMICRO LTD. All rights reserved.

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 Trademark Attributions

Qualcomm® is a trademark of Qualcomm Incorporated.

Bluetooth® is a trademark of the Bluetooth SIG, Inc.

Wi-Fi® is a trademark of the Wi-Fi Alliance.

AIRETOS® and OxfordTEC® are trademarked product brands of the VOXMICRO Group.

CVE is a registered trademark of The MITRE Corporation.

All other trademarks, trade names, and product names referenced herein are the property of their respective owners.

Revision History

Rev	Date	Change Summary	Author	Approved By	Evidence ID
A	March 16, 2026	Initial release	Product Management	Management / Legal	—

Table of Contents

NOTICE	2
Revision History	3
Table of Contents	4
1. PURPOSE AND SCOPE	6
1.1 Purpose	6
1.2 Scope of Products Covered	6
1.3 Regulatory Basis	6
2. REPORTING A VULNERABILITY	6
2.1 Single Point of Contact	6
2.2 What to Include in a Report	6
2.3 Encryption (Optional)	7
2.4 What is NOT in Scope	7
3. RESPONSE PROCESS	7
3.1 Acknowledgment	7
3.2 Triage and Assessment	7
3.3 Severity Classification (CVSS 3.1)	8
3.4 Remediation Objectives	8
3.5 Communication During Remediation	8
4. DISCLOSURE POLICY	8
4.1 Coordinated Disclosure Timeline	8
4.2 Embargo Period	8
4.3 Public Advisory	9
4.4 CVE Assignment	9
5. SECURITY UPDATE DELIVERY	9
5.1 Supply Chain Role	9
5.2 Firmware/BSP Update Process	9
5.3 Support Period Commitment	9
5.4 Update Availability Guarantee	9
5.5 Upstream Dependency	10
5.6 Rollback and Recovery	10

6. REGULATORY COMPLIANCE	10
6.1 EU CRA Reporting Obligations	10
6.2 CSIRT/ENISA Notification Procedures	10
6.3 Cross-Border Coordination	10
7. RESEARCHER RECOGNITION	10
7.1 Acknowledgment and Credit	10
7.2 Hall of Fame	11
7.3 Safe Harbor Statement	11
8. THIRD-PARTY COMPONENTS	11
8.1 Upstream Vendor Coordination	11
8.2 OEM Customer Notification	11
8.3 Supply Chain Communication	11
9. POLICY REVIEW AND UPDATES	11
9.1 Review Cadence	12
9.2 Change Notification	12
10. AUTHORIZED SIGNATORY	12

1. PURPOSE AND SCOPE

1.1 Purpose

VOXMICRO LTD ("VOXMICRO") is committed to the security of its products and welcomes vulnerability reports from security researchers, customers, and the general public. This policy describes how to report security vulnerabilities in AIRETOS and OxfordTEC products and how VOXMICRO will respond.

This Vulnerability Disclosure Policy ("VDP") establishes a coordinated framework for receiving, evaluating, remediating, and disclosing security vulnerabilities in VOXMICRO products and services.

1.2 Scope of Products Covered

This policy applies to:

- All AIRETOS wireless modules currently within their support period, across all product classes (E20, E92, E95, E98, C27, and future classes), all series (LGA, M.2 E-Key, M.2 B-Key, mPCIe), and all firmware/BSP versions under active support.
- OxfordTEC antenna products — limited to physical, connector, and integration issues. OxfordTEC products are passive components with no firmware; should future OxfordTEC products include active electronics, the full scope of this policy extends automatically.
- VOXMICRO web properties, including airetos.voxmicro.com and voxmicro.com.

1.3 Regulatory Basis

This policy is established in compliance with:

Regulation / Standard	Scope
Regulation (EU) 2024/2847 — Cyber Resilience Act (CRA)	Mandatory cybersecurity obligations for manufacturers of products with digital elements placed on the EU market
ISO/IEC 29147:2018 — Vulnerability Disclosure	International standard for external-facing vulnerability disclosure processes
ISO/IEC 30111:2019 — Vulnerability Handling Processes	International standard for internal vulnerability handling procedures

Effective date: March 16, 2026

2. REPORTING A VULNERABILITY

2.1 Single Point of Contact

To report a security vulnerability, contact VOXMICRO at:

- **Email:** vdp+security@voxmicro.com
- **Web form:** <https://www.voxmicro.com/security> (available upon deployment)

Reports submitted to this address are triaged by the VOXMICRO product security team. This mailbox is actively monitored during business hours and checked at least once daily outside business hours.

2.2 What to Include in a Report

To help VOXMICRO evaluate and respond effectively, please include:

- Product name and manufacturer part number (MPN)
- Firmware or BSP version (if applicable)
- A clear description of the vulnerability
- Steps to reproduce the issue
- Assessment of potential impact (if known)
- Your contact information (name or alias, email)

Detailed and well-structured reports enable faster triage and resolution. VOXMICRO appreciates the effort researchers invest in preparing quality reports.

2.3 Encryption (Optional)

Reporters may encrypt their submissions using VOXMICRO's PGP public key, available at:

<https://www.voxmicro.com/security/pgp-key.asc>

Encryption is recommended for reports containing sensitive technical details, proof-of-concept code, or information about actively exploited vulnerabilities.

2.4 What is NOT in Scope

The following are outside the scope of this policy:

- Social engineering attacks (phishing, pretexting) targeting VOXMICRO personnel
- Physical attacks requiring device access beyond normal intended use
- Denial-of-service attacks against VOXMICRO infrastructure
- Vulnerabilities in third-party services, platforms, or components not controlled by VOXMICRO
- Reports based on automated scanning tools without manual validation

3. RESPONSE PROCESS

3.1 Acknowledgment

VOXMICRO aims to acknowledge receipt of a vulnerability report within **5 business days**. The acknowledgment confirms that the report has been received and assigned for triage. VOXMICRO is a lean engineering organization; response times may vary with team availability.

3.2 Triage and Assessment

Following acknowledgment, VOXMICRO will endeavour to:

- Attempt to reproduce the reported vulnerability
- Validate the report against the affected product(s)
- Assess severity using the Common Vulnerability Scoring System (CVSS 3.1)
- Assign an internal tracking reference

The reporter will be informed of the triage outcome and preliminary severity assessment.

3.3 Severity Classification (CVSS 3.1)

Vulnerabilities are classified using CVSS 3.1 base scores:

Severity	CVSS Score	Response Priority
Critical	9.0 — 10.0	Immediate escalation; remediation prioritized
High	7.0 — 8.9	Priority remediation
Medium	4.0 — 6.9	Scheduled remediation
Low	0.1 — 3.9	Addressed in next maintenance release

3.4 Remediation Objectives

The following timelines are **objectives** reflecting industry best practice, not contractual commitments. Actual timelines depend on vulnerability complexity, upstream vendor coordination, and engineering capacity.

Phase	Objective	Notes
Acknowledgment	5 business days	Receipt confirmation and triage assignment
Triage and validation	Best effort	Reproduce, validate, assign CVSS score
Fix development (VOXMICRO-authored code)	Prioritized by severity	Critical/High prioritized; Medium/Low scheduled
Fix integration (upstream chipset firmware)	Dependent on IC vendor patch availability	VOXMICRO's integration begins upon receipt of upstream fix
Security update release	Without undue delay after validation	Per CRA: security updates made available to OEM customers free of charge
Public advisory	After embargo period or fix release	Whichever occurs later; see Section 4

Vulnerabilities originating in upstream IC vendor chipset firmware are dependent on the vendor's patch release cycle; VOXMICRO's integration and validation work for such issues begins upon receipt of the upstream fix. In all cases, VOXMICRO will communicate the expected timeline to the reporter and provide periodic status updates.

3.5 Communication During Remediation

VOXMICRO will provide the reporter with status updates at reasonable intervals while a vulnerability is under active remediation. Updates will include current progress, expected timeline adjustments, and any dependencies on upstream vendor coordination.

4. DISCLOSURE POLICY

4.1 Coordinated Disclosure Timeline

VOXMICRO follows coordinated vulnerability disclosure in accordance with ISO/IEC 29147:2018. Disclosure is coordinated between VOXMICRO, the reporter, and any affected third parties to minimize risk to end users.

4.2 Embargo Period

The default embargo period is **90 calendar days** from the date a security update becomes available. This window allows customers and integrators time to deploy updates before public disclosure.

Early disclosure may occur if:

- The vulnerability is already publicly known
- The vulnerability is actively exploited in the wild
- The reporter and VOXMICRO mutually agree to earlier disclosure

4.3 Public Advisory

Following the embargo period, VOXMICRO will publish a plain-language security advisory at:

<https://www.voxmicro.com/security/advisories/>

Advisories include: a description of the vulnerability, affected products and firmware versions, severity rating, remediation steps, and credit to the reporter (unless anonymity is requested).

4.4 CVE Assignment

VOXMICRO will request CVE identifiers for confirmed vulnerabilities through the CVE Program (via MITRE or a partner CVE Numbering Authority). CVE IDs are referenced in all public advisories to enable standardized tracking.

5. SECURITY UPDATE DELIVERY

5.1 Supply Chain Role

VOXMICRO is a B2B component manufacturer. AIRETOS wireless modules are integrated by OEM customers into their end products. Within this supply chain, VOXMICRO's security update obligation is to **make validated firmware and BSP updates available to its OEM customers** — not to deliver updates to end-users of OEM products. OEM integrators bear responsibility for incorporating module-level updates into their own product firmware and distributing them to their end-users.

This mirrors the established industry model in which IC vendors (such as Qualcomm) develop security patches and share them with module manufacturers, who in turn validate, integrate, and make them available to OEM customers downstream.

5.2 Firmware/BSP Update Process

Security updates for AIRETOS wireless modules are made available as firmware and/or BSP (Board Support Package) updates through existing customer channels, including direct download and the VOXMICRO engineering support portal. OEM customers are notified of available security updates and strongly recommended to deploy them in their released products as soon as possible.

5.3 Support Period Commitment

VOXMICRO commits to a minimum **5-year** security update support period from the date of each product class's market introduction, in accordance with EU CRA Article 13(6). During this period, VOXMICRO will monitor upstream IC vendor security bulletins, assess applicability to AIRETOS modules, and make validated updates available to OEM customers without delay.

5.4 Update Availability Guarantee

Security updates remain available for download for a minimum of **10 years** from the date of initial publication, or for the duration of the support period, whichever is longer, in accordance with EU CRA requirements.

5.5 Upstream Dependency

Security updates addressing vulnerabilities in IC vendor chipset firmware are dependent on the upstream vendor's patch availability. VOXMICRO's remediation timelines (Section 3.4) begin upon receipt of the upstream patch. Where upstream patches are delayed, VOXMICRO will communicate the dependency and expected timeline to affected OEM customers and, where possible, implement interim mitigations at the BSP or configuration level.

5.6 Rollback and Recovery

Rollback procedures for firmware and BSP updates are documented in product-specific release notes. Should a security update introduce a regression, VOXMICRO will provide a corrective update or documented rollback procedure without delay.

All security updates are provided free of charge. Where technically feasible, security updates are delivered separately from feature updates to simplify deployment and reduce risk.

6. REGULATORY COMPLIANCE

6.1 EU CRA Reporting Obligations

Effective **September 11, 2026**, VOXMICRO will comply with the EU Cyber Resilience Act (Regulation (EU) 2024/2847) vulnerability reporting obligations:

Reporting Milestone	Deadline
Early warning (actively exploited vulnerability detected)	Within 24 hours to national CSIRT and ENISA
Full notification (detailed vulnerability report)	Within 72 hours to national CSIRT and ENISA
Final report (after corrective measure available)	Within 14 days (actively exploited) or 1 month (severe incidents)

6.2 CSIRT/ENISA Notification Procedures

Mandatory vulnerability reports are submitted through the **EU CRA Single Reporting Platform (SRP)**, operated by ENISA.

VOXMICRO's designated national CSIRT is **GR-CSIRT (National CERT of Greece)**, corresponding to VOXMICRO LTD's main EU establishment in Greece.

Should the ENISA SRP not be operational at the time a report is required, VOXMICRO will submit reports directly to GR-CSIRT and ENISA through available interim channels.

6.3 Cross-Border Coordination

Where a vulnerability affects products distributed across multiple EU Member States, VOXMICRO will coordinate with the relevant national CSIRTs through the ENISA-facilitated cross-border notification framework.

7. RESEARCHER RECOGNITION

7.1 Acknowledgment and Credit

All reporters who submit valid vulnerability reports are credited by name (or alias of their choice) in the published security advisory, unless the reporter requests anonymity.

7.2 Hall of Fame

VOXMICRO maintains a public acknowledgment page at:

<https://www.voxmicro.com/security/acknowledgments/>

Credited researchers are listed with the advisory reference, date, and a brief description of their contribution.

7.3 Safe Harbor Statement

VOXMICRO will not pursue legal action against individuals who:

- Discover and report security vulnerabilities in good faith and in compliance with this policy
- Avoid intentional harm to VOXMICRO systems, data, employees, or customers during their research
- Do not exploit a vulnerability beyond the minimum necessary to demonstrate its existence
- Allow VOXMICRO a reasonable period to address the vulnerability before any public disclosure
- Do not violate applicable law in the course of their research

Good-faith security research conducted in accordance with this policy is considered authorized conduct. VOXMICRO will not initiate or support legal proceedings against researchers who comply with these terms.

VOXMICRO is evaluating structured vulnerability intake platforms (such as HackerOne) and a potential bug bounty program, and welcomes expressions of interest from the security research community.

8. THIRD-PARTY COMPONENTS

8.1 Upstream Vendor Coordination

Vulnerabilities affecting IC vendor chipset firmware or other third-party components integrated into AIRETOS modules will be reported upstream through the respective vendor's Product Security Incident Response Team (PSIRT) channels. VOXMICRO will coordinate disclosure timing with upstream vendors to ensure patches are available across the supply chain before public disclosure.

8.2 OEM Customer Notification

OEM customers deploying AIRETOS modules in their products will be notified of critical and high-severity vulnerabilities via direct communication prior to public advisory publication. This advance notification enables OEM integrators to plan and coordinate patch deployment within their own products and release schedules.

8.3 Supply Chain Communication

VOXMICRO participates in coordinated multi-party disclosure when a shared component vulnerability affects multiple manufacturers. This includes participation in coordinated response efforts facilitated by upstream vendors, CERTs, and industry coordination bodies.

9. POLICY REVIEW AND UPDATES

9.1 Review Cadence

This policy is reviewed at minimum **annually**, and additionally upon:

- Publication of EU CRA implementing acts or delegated regulations
- Material changes to ENISA coordinated vulnerability disclosure guidance
- Significant changes to VOXMICRO's product portfolio or security infrastructure
- Lessons learned from vulnerability handling experience

9.2 Change Notification

Material changes to this policy will be announced at:

<https://www.voxmicro.com/security/>

Where possible, VOXMICRO will provide **30 calendar days** advance notice of material policy changes. This policy is maintained under VOXMICRO Documentation Protocol revision control with alphabetical revision identifiers.

10. AUTHORIZED SIGNATORY

Signed for and on behalf of VOXMICRO LTD.

Place and date of issue: 20955 Pathfinder Road, STE100 91765 Diamond Bar, California United States of America

Date: March 16, 2026



This document is subject to the Protocol Revision Policy. Any revision must reproduce all sections in their complete, unabridged form.