Security & Vulnerability Disclosure Policy

The **Cyber Resilience Act (CRA)** is a landmark European Union regulation establishing mandatory cybersecurity requirements for hardware and software products with digital elements placed on the EU market. By addressing vulnerabilities throughout the entire product lifecycle, the CRA aims to protect consumers and businesses from cyber threats, ensuring that “security by design” becomes the baseline standard for connected devices.

Key Pillars of the CRA:

- **Security by Design & Default:** Products must be developed and delivered with optimal security configurations, minimizing the attack surface from day one.
- **Life-Cycle Vulnerability Management:** Manufacturers are required to monitor, identify, and address vulnerabilities, providing regular security updates for a minimum specified period (or the expected lifetime of the product).
- **Transparency & Compliance:** Clear documentation and information must be provided to end-users regarding the product’s security features and support duration.
- **Duty to Report:** Active exploitation of vulnerabilities or severe security incidents must be reported to national authorities and ENISA within strict timeframes.

NiLAB GmbH is committed to ensuring the security of the products and software we develop, including our linear motor drives (NLi and GDi families) and the NiLAB Starter configuration software.We value the work of security researchers and customers who help us identify and address potential vulnerabilities, and we are committed to working with them in a coordinated and constructive way.

Scope

This policy covers vulnerabilities affecting:
• NiLAB integrated-drive linear motors (NLi, GDi families) and their firmware
• NiLAB Starter (Windows configuration software)
If you are uncertain whether an issue falls within this scope, please report it anyway — we would rather review a report that turns out to be out of scope than miss a real issue.

Important Notice

The availability of this vulnerability reporting channel is intended to support responsible and coordinated vulnerability disclosure. The availability of this reporting channel does not imply certification, security guarantees, or compliance claims regarding any specific product, software, firmware, or service provided by **NiLAB GmbH**. NiLAB continuously evaluates and improves the cybersecurity features of its products and services as part of its product security and vulnerability management processes.All reported issues will be assessed and handled according to NiLAB's cybersecurity processes and vulnerability management procedures.

How to report a vulnerability

Please report potential security vulnerabilities using our online reporting form:
https://www.ni-lab.online/SRF/report-vulnerability.php

When submitting a report, please include as much of the following information as possible:
• The affected product, model, and firmware/software version
• A description of the vulnerability and its potential impact
• Steps to reproduce the issue, or a proof of concept, if available
• Whether you believe the vulnerability is being actively exploited
• Your contact details, if you would like to be kept informed of progress (reports can also be submitted without contact details)

What to expect from us

• Acknowledgement: we aim to confirm receipt of your report within 3 business days after submission.
• Triage and investigation: our team will assess the report, determine its validity and severity, and keep you informed of progress where contact details are provided.
• Coordinated disclosure: we ask that you do not publicly disclose details of a reported vulnerability until we have had the opportunity to investigate and, where applicable, make a fix available. We will work with you to agree on a reasonable disclosure timeline.
• Remediation: once a vulnerability is confirmed, we will work to address it through a security update or other appropriate mitigation, and will provide affected customers with relevant information and guidance.
• Public disclosure: once a fix is available, we will publish information about the resolved vulnerability,

including a description of the issue and the affected products, in line with our obligations under applicable regulations
(including the EU Cyber Resilience Act: https://digital-strategy.ec.europa.eu/en/policies/cra-summary).

Confidentiality

NiLAB GmbH will treat vulnerability reports and any associated technical information as confidential and will use such information solely for the purpose of investigating, validating, mitigating, and remediating reported security issues.

Responsible testing guidelines

When researching potential vulnerabilities, we ask that you:
• Avoid actions that could harm the reliability or integrity of our systems, products, or data, or that of our customers (for example, avoid testing on production systems controlling physical equipment without prior coordination with us)
• Do not access, modify, or delete data that does not belong to you
• Give us a reasonable opportunity to investigate and address an issue before any public disclosure
• Act in good faith and comply with applicable laws
We will not pursue legal action against researchers who act in good faith and in accordance with this policy.

Contact

For questions about this policy, or if the reporting form is unavailable, you can contact us at:
katharina.pirker@nilab.at

This policy forms part of NiLAB GmbH's cybersecurity governance framework and supports our ongoing preparations and obligations under the EU Cyber Resilience Act (Regulation (EU) 2024/2847).

Security Contact Information

NiLAB may additionally publish security contact information through a security.txt file in accordance with RFC 9116.