Security & Vulnerability Disclosure Policy [DRAFT]

NiLAB GmbH is committed to ensuring the security of the products and software we develop, including our linear motor drives (NLi, NL, GD, 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.

How to report a vulnerability

Please report potential security vulnerabilities using our online reporting form:
Report a vulnerability: [link to be added]

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 a reasonable time 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).

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 is part of NiLAB GmbH's commitment to product security under the EU Cyber Resilience Act (Regulation (EU) 2024/2847).