

Vulnerability Disclosure Policy for Novotechnik products with digital features

1 Purpose and Scope

Novotechnik Messwertaufnehmer OHG (Novotechnik for short) operates a coordinated process for receiving, assessing, addressing, and responsibly disclosing vulnerabilities in products with digital components that are developed, manufactured, or marketed under Novotechnik's own brand. This policy currently applies to products with the customer interfaces CANopen, CAN J1939, and IO-Link. The goal is to identify risks early, adequately protect those affected, and implement necessary measures in a transparent manner.

This policy governs the reporting and coordinated disclosure of product vulnerabilities to Novotechnik, as well as the provision of information to affected users. Novotechnik's legal obligations to report, provide information, and cooperate with competent authorities or reporting agencies remain unaffected by this policy and may be fulfilled independently of the coordinated public disclosure.

General IT security incidents, data protection inquiries, physical product defects, and support requests unrelated to cybersecurity are not covered by this policy.

2 Information Required for a Report

The following information is required for the efficient handling and assessment of the vulnerability by PSIRT:

- Product/Model Name, Part Number, and Hardware and Firmware/Software Version
- Description of the observed behavior, affected interface, and potential security implications in the customer application
- Reproducible steps, operating environment, required permissions, or physical access
- Technical information, such as log files, bus traces, or screenshots, if available
- Contact information for questions and feedback, if desired
- Known CVE or CWE references, if available
- Information regarding a planned or previous disclosure of the vulnerability

Providing contact information is voluntary. Anonymous reports are also reviewed to the extent possible. However, without contact information, Novotechnik cannot follow up with questions or provide updates on the status of the report. In the case of a report classified as serious, Novotechnik stores the provided contact information, if available, in its internal reporting database. This database is maintained in accordance with the provisions of the General Data Protection Regulation (GDPR). Novotechnik's privacy policy can be found at <https://www.novotechnik.de/en/privacy-policy/>.

For the transmission of confidential technical information, we recommend encryption using the public PGP key published on our PSIRT website. Please do not transmit passwords, private keys, production access credentials, or confidential customer data in unencrypted form.

3 PSIRT Vulnerability Management Process at Novotechnik

No.	Step	Novotechnik-Activity
1	Receipt	Document the report, assign a reference number, take the need for protection into account, and confirm receipt within a few business days.
2	Validation and Evaluation	Reproduce the vulnerability, collect evidence, identify the affected products, versions, and components, and assess the reported vulnerability.
3	Procedure und Verification	Coordination with Product Development to develop corrective actions. If necessary, corrections or corrective actions will be reviewed and made available to you, as the person who reported the issue, for your review.
4	Disclosure and Closure	Risk-based customer notification or publication of a security advisory following verification of appropriate corrective, remedial, or protective measures. As part of a coordinated disclosure, the reporter may be named in the security advisory upon request and following prior consultation.

4 Risk Assessment and Remedial Action

Die Prioritization is risk-based. Novotechnik takes into account, in particular, the technical severity, attack prerequisites, indications of active exploitation, affected product versions, and potential impacts on availability, integrity, confidentiality, and authenticity.

Potential safety or system-related consequences are taken into account to the extent that

Novotechnik has the necessary information regarding the customer's application. A CVSS base score alone is not the sole determining factor for the type and scope of the measures taken.

5 Policy on the Disclosure of Vulnerabilities

Once a corrective measure has been provided, Novotechnik generally publishes a security advisory regarding the resolved vulnerability. To the extent necessary and appropriate for safe use, this advisory contains information on the affected products and versions, the potential impacts and severity, as well as available security updates, workarounds, or other protective measures.

If the risks associated with immediate publication outweigh the benefits of public disclosure, Novotechnik may reasonably delay the public release of certain information until affected users have had the opportunity to implement the intended corrective measures.

Novotechnik treats all received vulnerability reports and the identity of the reporter as confidential and discloses information only to the extent necessary for processing, remediation, coordination, or compliance with legal obligations.

For further questions or feedback, please contact us via email at psirt@novotechnik.de