Coordinated vulnerability disclosure policy

Cybersecurity is a high priority for us. The security of our products and components is an essential part of our quality commitment. Despite careful development, testing, and quality assurance measures, security vulnerabilities cannot be completely ruled out.

We therefore welcome reports of potential vulnerabilities and support responsible, coordinated vulnerability disclosure. By reporting, you help us continuously improve the security of our products.

1 Which reports do we accept?

We welcome reports of potential vulnerabilities as well as security incidents relating to our products or components. In particular, these include reports on:

- vulnerabilities in our products with digital elements (software, hardware firmware),
- vulnerabilities in libraries and integrated third-party components,
- observed or suspected security incidents that affect or may affect the cybersecurity or safe operation of our products.

Wherever possible, please report vulnerabilities and security incidents that concern our products, components, or the associated infrastructure, are not yet publicly known, and can be substantiated by a clear description or appropriate evidence. Pure results of automated scans without additional explanations generally cannot be processed.

General product defects without a security relevance, feature requests, and support inquiries are not covered by this policy.

2 How can you report a vulnerability or a security incident?

If you have identified a vulnerability or a security-relevant incident in connection with our products, please send us an email to: security@cetoni.de

To enable a quick processing, we ask you to provide as much of the following information as possible:

- affected product or component
- product or software version
- description of the vulnerability, or description of the observed behavior in the case of security incidents (including time of observation)
- steps to reproduce
- Proof of Concept (if available)
- assessment of possible impact
- known CVE number or references (if applicable)
- indication of whether the vulnerability has already been exploited

The more complete your information is, the faster we can evaluate your report.

3 Our handling of your report

After receiving your report, we will:

- acknowledge receipt within 5 working days,
- check the report for plausibility and relevance,
- technically assess the vulnerability or security incident,
- contact you in case of follow-up questions,
- develop appropriate countermeasures, and
- inform affected customers and, where applicable, the competent authorities in accordance with legal requirements.

During processing, we endeavor to maintain reasonable communication about the progress.

4 Responsible Disclosure

We ask you to:

- allow us sufficient time to analyze and remediate the reported vulnerability,
- publicly disclose details of the vulnerability only after agreeing with us or after publication of a suitable countermeasure,
- not perform any actions that impair the operation of our systems or the availability of our products,
- not access, modify, or publish personal data without authorization.

5 Privacy Policy

Personal data that you provide when submitting your report will be used exclusively to process your vulnerability report and will be handled in accordance with applicable data protection regulations.

6 Our Promise

We treat all reports confidentially and solely for the purpose of assessing and remediating the reported vulnerability.

If you act in accordance with this policy and proceed in good faith, we will not initiate any legal proceedings based on your vulnerability report.

We explicitly thank you for your support in improving our product security.