

RP-Technik GmbH

Hermann-Staudinger-Str. 10-16
63110 Rodgau
Germany

Tel. +49 6106 660 28-0
Fax +49 6106 660 28-40
E-mail: info@rp-group.com
www.rp-group.com

VAT ID No.: DE296414578

Rodgau, September 11, 2026

Coordinated Vulnerability Disclosure (CVD) Policy of RP-Technik GmbH

As a manufacturer of products with digital elements, we take the cybersecurity of our systems and products very seriously. In accordance with the requirements of the EU Cyber Resilience Act (Regulation 2024/2847), Annex I, Part II, Nos. 5 & 6, we have established this Coordinated Vulnerability Disclosure (CVD) policy. The aim is to provide security researchers and third parties with a transparent and secure way to report potential vulnerabilities to us. If you have discovered a security vulnerability in our systems or products, please report it to us confidentially via the reporting channel described below. This will allow us to resolve the issue without harming others.

1. Scope

This policy applies to:

- All hardware and software products developed, distributed and actively supported by us, as well as
- our official online services and infrastructures that are directly linked to the function or delivery of our digital products.
- The following are excluded from the scope of this directive:
 - Third-party products that are not integrated into a product of RP Technik GmbH;
 - general IT equipment and tools on/with which products of RP Technik GmbH are operated;
 - customer-side installations and systems of customers, partners and operators.

2. Central Reporting Office (Single Point of Contact)

Reports of potential vulnerabilities can be submitted to our responsible team (Product Security Incident Response Team, PSIRT) via the following channels:

- **E-mail:** security@rp-group.com
- **Encryption:** Please encrypt sensitive data using our PGP key. <https://www.rp-group.com/well-known/pgp-key.txt>
- **security.txt:** You can always find our standardized contact details in machine-readable format at <https://www.rp-group.com/well-known/security.txt> according to RFC 9116.

3. Expected Behavior & Submission

To help us with coordinated treatment, we ask that you provide as much information as possible when reporting an incident:

- Which product is affected (name, URL if applicable, version, e.g. Core-Bus Slave Module v1.4),
- detailed description of the vulnerability, whether it is a discovered vulnerability or an actual security incident,
- how the vulnerability was found and what potential impact it has on your business,
- date and time (if possible, including time zone) of discovery of the vulnerability or incident,
- location of the installation (including country) where the product is used, as well as
- indications of possible malicious activity (e.g., unauthorized access).
- Please also attach any relevant screenshots or log files to your message that could help us understand the issue.
- The preferred processing language is German or English. Please submit your report in one of these languages.

Note: This policy does not create any entitlement to financial compensation or bonuses. It also does not establish any contractual relationship or enforceable claim by third parties to specific processing results, deadlines, compensation, acknowledgments, or publication.

4. Our Commitment & Timeline

We are committed to the professional and transparent processing of every valid report.:

1. **Confirmation of receipt:** You will receive confirmation of receipt of your report and a ticket reference number within 3 working days, unless the report was submitted anonymously.
2. **Validation (Triage):** We will examine and assess the vulnerability as quickly as possible (usually within 5-10 working days) and inform you of the result.
3. **Solution:** We are working with high priority to provide a security update or appropriate risk mitigation measures.
4. **Coordinated Disclosure:** We will coordinate the timing of the security advisory publication with you. By default, we aim for a remediation within 90 days prior to public notification. If this timeframe is insufficient for remediation, we will extend it once by an additional 90 days in consultation with the responsible national CSIRT. The notification will be submitted at least via the European Vulnerability Database (EUVD) of ENISA; in Germany, CERT-Bund is the responsible national CSIRT.
5. **Personal data:** We will only pass this information on to third parties with your explicit consent.

5. Safe Harbor (Legal Protection for Researchers) & Our Expectations

We greatly value the work of security researchers. If you adhere to the following principles in your analyses and reporting, we will not initiate or support any civil or criminal legal action against you:

- You do not actively interfere with our customers' production systems and do not disrupt their operations, e.g. through brute-force or denial-of-service attacks, etc.
- You do not exploit the vulnerability (e.g., no reading or modifying customer data, no extortion, no distribution of tools to exploit the reported vulnerability on darknet markets).
- You will only disclose the vulnerability to third parties once a corresponding security update has been provided by us or the coordination period agreed between us has expired (Coordinated Disclosure).

- Your actions do not violate applicable law outside of pure, non-destructive vulnerability detection.

We expect that your vulnerability report contains previously unknown information. While we will accept and review your information regarding vulnerabilities that have already been resolved, this information does not qualify for further processing within the CVD process. We also reserve the right not to respond to a large number of irrelevant and unusable reports.

You may also submit your report anonymously. We do not require a non-disclosure agreement (NDA). However, we ask that you provide valid contact information (email address) in your report so that we can contact you if we have any questions. Especially with complex vulnerabilities, it is possible that we will need further explanations and documentation. Since we place great importance on good communication, reports without the opportunity for consultation may only be processed to a limited extent.

A notice: This policy can also be found via our machine-readable file security.txt according to RFC 9116 at www.rp-group.com/well-known/security.txt, field "Policy:".