

RP-Technik GmbH

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

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

USt-IdNr.: DE296414578

Rodgau, 11. September 2026

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

Als Hersteller von Produkten mit digitalen Elementen nehmen wir die Cybersicherheit unserer Systeme und Produkte sehr ernst. In Übereinstimmung mit den Anforderungen des EU Cyber Resilience Act (Verordnung 2024/2847), Anhang I, Teil II, Nr. 5 & 6, haben wir diese Richtlinie zur koordinierten Offenlegung von Schwachstellen (CVD) etabliert. Ziel ist es, Sicherheitsforschern und Dritten einen transparenten Weg zu bieten, potentielle Schwachstellen sicher an uns zu übermitteln. Wenn Sie eine Sicherheitslücke in unseren Systemen oder Produkten entdeckt haben, bitten wir Sie, uns diese durch unsere nachfolgend beschriebene Meldestelle vertraulich zu melden. So können wir das Problem beheben, ohne dass andere davon Schaden nehmen.

1. Geltungsbereich (Scope)

Diese Policy gilt für:

- Alle von uns entwickelten, vertriebenen und aktiv unterstützten Hardware- und Softwareprodukte sowie
- unsere offiziellen Onlinedienste und Infrastrukturen, die direkt mit der Funktion oder Bereitstellung unserer digitalen Produkte verknüpft sind.
- Ausgenommen vom Anwendungsbereich dieser Richtlinie sind:
 - Produkte Dritter, die nicht in ein Produkt der RP Technik GmbH integriert sind;
 - allgemeine IT-Geräte, und Tools an/mit denen Produkte der RP Technik GmbH betrieben werden;
 - kundenseitige Installationen und Systeme von Kunden, Partnern und Betreibern.

2. Zentrale Meldestelle (Single Point of Contact)

Berichte über potentielle Schwachstellen können über folgende Kanäle an unser zuständiges Team (Product Security Incident Response Team, PSIRT) übermittelt werden:

- **E-Mail:** security@rp-group.com
- **Verschlüsselung:** Bitte verschlüsseln Sie sensible Daten mit unserem PGP-Schlüssel <https://www.rp-group.com/well-known/pgp-key.txt>
- **security.txt:** Unseren standardisierten Kontaktpfad finden Sie stets maschinenlesbar unter <https://www.rp-group.com/well-known/security.txt> gemäß RFC 9116.

Authorized Representatives Executive Director:
Reinald Pasedag, Roland Pasedag, Oliver Meinicke
Steuer-Nr. 044 242 60907
WEEE-Reg.Nr. DE 52317483
District Court Offenbach HRB 47929

Place of Jurisdiction:
Seligenstadt/Main

Company Headquarters:
Rodgau

Bank Details:
Sparkasse Dieburg
BIC: HELADEF1DIE
IBAN: DE92 5085 2651 0155 0125 03

3. Erwartetes Verhalten & Einreichung

Um eine koordinierte Behandlung zu ermöglichen, bitten wir Sie bei einer Meldung um möglichst vollständige Informationen:

- Welches Produkt betroffen ist (Name, ggf. URL, Version, z. B. Core-Bus Slave Modul v1.4),
- detaillierte Beschreibung der Schwachstelle, ob es sich um eine gefundene Schwachstelle oder einen tatsächlichen Sicherheitsvorfall handelt,
- wie die Schwachstelle gefunden wurde und welche potentiellen Auswirkungen sie auf Ihren Betrieb hat,
- Datum und Uhrzeit (wenn möglich, inkl. Zeitzone) der Entdeckung der Schwachstelle oder des Vorfalls,
- Standort der Installation (inkl. Land), wo das Produkt eingesetzt wird, sowie
- Hinweise auf eventuelle böswillige Aktivitäten (z.B. unbefugte Zugriffe).
- Fügen Sie Ihrer Nachricht bitte auch evtl. relevante Screenshots oder Log-Dateien bei, die uns beim Nachvollziehen helfen können.
- Die bevorzugte Bearbeitungssprache ist Deutsch oder Englisch. Bitte reichen Sie Ihre Meldung in einer dieser Sprachen ein.

Hinweis: Diese Richtlinie begründet keinen Anspruch auf finanzielle Vergütung oder Prämien. Sie begründet auch kein Vertragsverhältnis und keinen durchsetzbaren Anspruch Dritter auf bestimmte Bearbeitungsergebnisse, Fristen, Vergütung, Danksagung oder Veröffentlichung.

4. Unsere Verpflichtung & Zeitplan (Timeline)

Wir verpflichten uns zur professionellen und transparenten Bearbeitung jeder validen Meldung:

1. **Eingangsbestätigung:** Sie erhalten innerhalb von **3 Werktagen** eine Bestätigung über den Erhalt Ihrer Meldung sowie ein Ticket-Aktenzeichen, sofern die Meldung nicht anonym erfolgte.
2. **Validierung (Triage):** Wir prüfen und bewerten die Schwachstelle schnellstmöglich (in der Regel innerhalb von 5–10 Werktagen) und informieren Sie über das Ergebnis.
3. **Behebung:** Wir arbeiten mit hoher Priorität an der Bereitstellung eines Sicherheitsupdates oder geeigneten Risikominderungsmaßnahmen.
4. **Koordinierte Offenlegung:** Wir stimmen den Zeitpunkt der Veröffentlichung der Sicherheitswarnung (Security Advisory) mit Ihnen ab. Standardmäßig streben wir eine Behebung innerhalb von 90 Tagen vor der öffentlichen Bekanntmachung an. Reicht diese Zeit für die Behebung nicht aus, verlängern wir einmalig um weitere 90 Tage in Abstimmung mit dem zuständigen nationalen CSIRT. Die Meldung erfolgt mindestens über die European Vulnerability Database (EUVD) der ENISA; in Deutschland ist CERT-Bund das zuständige nationale CSIRT.
5. **Personenbezogene Daten** werden wir nur mit Ihrer ausdrücklichen Zustimmung an Dritte weitergeben.

5. Safe Harbor (Rechtlicher Schutz für Forscher) & unsere Erwartungen

Wir schätzen die Arbeit von Sicherheitsforschern außerordentlich. Wenn Sie bei Ihren Analysen und der Meldung die folgenden Grundsätze einhalten, werden wir keine zivil- oder strafrechtlichen Schritte gegen Sie einleiten oder unterstützen:

- Sie greifen nicht aktiv in Produktivsysteme unserer Kunden ein und beeinträchtigen nicht deren Betrieb, z.B. durch Brute-Force- oder Denial-of-Service-Angriffe etc..
- Sie nutzen die Schwachstelle nicht aus (z.B. kein Auslesen oder Verändern von Kundendaten, kein Erpressungsverhalten, keine Verbreitung von Tools zur Ausnutzung der gemeldeten Schwachstelle auf Darknet-Märkten).
- Sie legen die Schwachstelle Dritten erst dann offen, wenn ein entsprechendes Sicherheitsupdate von uns bereitgestellt wurde oder die zwischen uns vereinbarte Koordinationsfrist abgelaufen ist (Coordinated Disclosure).
- Ihre Handlungen verstoßen nicht gegen geltendes Recht außerhalb der reinen, zerstörungsfreien Schwachstellensuche.

Wir erwarten, daß es sich bei Ihrer Schwachstellenmeldung um bisher nicht bekannte Informationen handelt. Zu bereits behobenen Schwachstellen werden Ihre Informationen zwar entgegengenommen und geprüft, sie qualifizieren sich jedoch nicht für eine weiterführende Bearbeitung im Rahmen des CVD-Prozesses. Wir behalten uns weiterhin vor, auf eine große Anzahl irrelevanter und unbrauchbarer Meldungen nicht zu reagieren.

Ihre Meldung darf auch anonym erfolgen. Wir verlangen keine Verschwiegenheitsvereinbarung (NDA). Wir bitten Sie jedoch, in Ihrer Meldung gültige Kontaktdaten (E-Mail-Adresse) anzugeben, damit wir Sie im Falle von Rückfragen kontaktieren können. Gerade bei komplexen Schwachstellen ist es nicht auszuschließen, dass wir weitere Erklärungen und Dokumentationen benötigen. Da wir großen Wert auf eine gute Kommunikation legen, werden Meldungen ohne Möglichkeit zur Rücksprache evtl. nur eingeschränkt bearbeitet.

Hinweis: Diese Policy ist auch über unsere maschinenlesbare Datei security.txt nach RFC 9116 auffindbar unter www.rp-group.com/well-known/security.txt, Feld „Policy:“.