



SCHRAML CRA Richtlinie zur koordinierten Offenlegung von Schwachstellen (CVD-Policy)

1. Zweck und Rechtsgrundlage

Die SCHRAML GmbH (SCHRAML) nimmt Hinweise auf Sicherheitslücken in ihren Produkten entgegen und bearbeitet sie koordiniert mit den Meldenden.

Diese Richtlinie dient der Umsetzung von Art. 13 Abs. 17 sowie Anhang I Teil II Nr. 5 und 6 der [Verordnung \(EU\) 2024/2847](#) des Europäischen Parlaments und des Rates vom 23. Oktober 2024 (Cyberresilienz-Verordnung, „CRA“). Sie orientiert sich an ISO/IEC 29147 und ISO/IEC 30111.

2. Geltungsbereich

Die Richtlinie gilt für alle nicht-abgekündigten Produkte mit digitalen Elementen, die SCHRAML in der EU bereitstellt, einschließlich Software, Firmware und zugehöriger Dienste.

Nicht erfasst sind Meldungen zu Phishing, Spam, Social Engineering oder Denial-of-Service. Diese richten Sie bitte an security@schraml.de. Meldungen ohne Sicherheitsbezug (z.B. Bugmeldungen) weiterhin bitte an info@schraml.de.

3. So melden Sie eine Schwachstelle

Kanal	Angabe
E-Mail	psirt@schraml.de
Verschlüsselung	OpenPGP-Schlüssel: https://www.schraml.de/.well-known/SCHRAML_psirt-pgp-key_public.asc Fingerprint: openpgp4fpr:185374FBCCD1BF93137A24AE12553FB363E92CC2
Alternativ	Postanschrift: SCHRAML GmbH PSIRT Herxheimer Str. 7 83620 Vagen
Sprachen	Deutsch, Englisch

Kanal	Angabe
Maschinenlesbar	/.well-known/security.txt

Bitte senden Sie vertrauliche Details verschlüsselt. Für große Anhänge stellen wir auf Anfrage einen sicheren Austauschkanal bereit.

Nutzen Sie gerne unser hierfür vorgesehenes Kontaktformular. Die Verschlüsselung erfolgt hier bereits.

Hilfreiche Angaben:

- Produkt und Version
- Beschreibung der Schwachstelle und mögliche Auswirkung
- Schritte zur Reproduktion, ggf. Proof of Concept
- Ihre Kontaktdaten und ob Sie namentlich genannt werden möchten

4. Ablauf und Reaktionszeiten

Die Zeiten sind Zielwerte, keine Garantien.

Schritt	Ziel
Eingangsbestätigung	innerhalb von 5 Werktagen
Erste Bewertung (evtl. CVSS)	innerhalb von 10 Werktagen
Statusupdates	mindestens alle 30 Tage
Behebung	abhängig vom Schweregrad, abgestimmt

Wird eine Schwachstelle aktiv ausgenutzt, erfüllen wir zusätzlich unsere Meldepflichten nach Art. 14 CRA gegenüber dem zuständigen CSIRT (BSI) und ENISA.

5. Koordinierte Offenlegung

Wir veröffentlichen Informationen zu behobenen Schwachstellen in Abstimmung mit Ihnen, in der Regel spätestens 90 Tage nach Eingang der Meldung. Die Frist kann einvernehmlich angepasst werden, etwa wenn Kunden Zeit für die Installation von Updates in Anlagen benötigen.

Sicherheitshinweise (Advisories) veröffentlichen wir unter <https://www.schraml.de/index.php/security-advisories/>, maschinenlesbar im CSAF-Format.

6. Regeln für Meldende

Bitte:

- testen Sie nur an eigenen Systemen oder Testinstallationen, nie an produktiven Anlagen von Kunden
- greifen Sie nicht auf Daten Dritter zu und verändern oder löschen Sie keine Daten
- beeinträchtigen Sie nicht den Betrieb von Systemen
- veröffentlichen Sie keine Details vor abgestimmter Offenlegung

7. Unsere Zusagen

Wenn Sie in gutem Glauben und im Rahmen dieser Richtlinie handeln, werden wir keine rechtlichen Schritte gegen Sie einleiten und keinen Strafantrag stellen. Die Befugnisse von Strafverfolgungsbehörden und Rechte Dritter können wir damit nicht einschränken.

Wir behandeln Ihre Meldung vertraulich und geben Ihre Daten nur mit Ihrer Zustimmung weiter, soweit keine gesetzliche Pflicht besteht.

8. Danksagung

Auf Wunsch nennen wir Sie im Advisory.

9. Weitere Hinweise

Datenschutz: Wir verarbeiten Ihre Angaben ausschließlich zur Bearbeitung der Meldung (Art. 6 Abs. 1 lit. f DSGVO). Details: <https://www.schraml.de/index.php/datenschutzerklaerung/>

Behördliche Meldestellen: Sie können Schwachstellen nach Art. 15 CRA auch freiwillig dem zuständigen CSIRT melden, in Deutschland dem [BSI](#).

Version: 1.0, Stand 09/2026. Wir passen diese Richtlinie bei Bedarf an.