Richtlinie zur koordinierten Offenlegung von Schwachstellen

Coordinated Vulnerability Disclosure (CVD) Policy
Version 1.0 | Stand 08.09.2026 | Kontakt: security@gemat.ch

1. Zweck

Die Sicherheit unserer Produkte ist uns wichtig. Diese Richtlinie beschreibt, wie Sie uns eine Sicherheitsschwachstelle melden können und wie wir damit umgehen. Wir begrüssen Meldungen von Sicherheitsforschenden, Kunden und Dritten.

2. Geltungsbereich

Diese Richtlinie gilt für Produkte mit digitalen Elementen, die Grossenbacher Automation AG unter eigenem Namen oder eigener Marke in Verkehr bringt.

Nicht erfasst: Produkte, die wir im Kundenauftrag fertigen und die unter dem Namen oder der Marke des Kunden vertrieben werden. Für diese ist der jeweilige Kunde als Hersteller verantwortlich; bitte richten Sie Meldungen an diesen bzw. an Ihren Systemlieferanten.

Unsere Produkte werden an gewerbliche Kunden geliefert und von diesen in eigene Maschinensteuerungen und -systeme integriert. Meldungen zu einem Gesamtsystem richten Sie bitte an den Hersteller des Gesamtsystems.

3. Wie Sie eine Schwachstelle melden

Bitte senden Sie Ihre Meldung an security@gemat.ch oder über das Meldeformular unter www.gemat.ch/de/cra-meldung. Meldungen bitte in Deutsch oder Englisch.

Hilfreiche Angaben: betroffenes Produkt und Version, Beschreibung der Schwachstelle und möglichen Auswirkung, Schritte zur Reproduktion sowie Hinweise auf eine etwaige aktive Ausnutzung.

4. Was Sie von uns erwarten können

- Wir bemühen uns, den Eingang Ihrer Meldung innerhalb von 5 Arbeitstagen zu bestätigen.
- Wir bewerten die Meldung (Triage) und nehmen eine Kategorisierung vor.
- Die Priorisierung richtet sich nach Auswirkung, Schweregrad und Ausnutzbarkeit. Feste Behebungsfristen sagen wir nicht zu.
- Wir bearbeiten und beheben soweit notwendig/angebracht die gemeldete Schwachstelle und informieren Sie über den Abschluss des Vorganges.

5. Koordinierte Offenlegung

Bitte veröffentlichen Sie Informationen zur Schwachstelle nicht, bevor wir uns über das Vorgehen abgestimmt haben. In der Regel erfolgt eine Veröffentlichung erst, wenn eine Korrektur- oder Minderungsmassnahme verfügbar ist. Den Zeitpunkt stimmen wir gemeinsam mit Ihnen ab.

6. Rahmen für Meldende

Bitte handeln Sie in gutem Glauben und halten Sie geltendes Recht ein. Insbesondere:

- greifen Sie nicht auf mehr Daten zu als nötig und verändern oder löschen Sie keine Daten;
- führen Sie keine Denial-of-Service-Tests durch und beeinträchtigen Sie den Betrieb nicht;
- kein Social Engineering und keine physischen Angriffe auf Personen oder Einrichtungen;
- verwenden Sie nur nicht-destruktive Proof-of-Concepts und geben Sie erlangte Daten nicht weiter.

7. Vergütung

Wir bieten für Meldungen keine finanzielle Vergütung (kein Bug-Bounty-Programm).

8. Änderungen

Wir können diese Richtlinie jederzeit anpassen. Massgeblich ist die jeweils veröffentlichte Fassung.

Grossenbacher Automation AG
Spinnereistrasse 10
CH-9008 St. Gallen

security@gemat.ch