Coordinated Vulnerability Disclosure Policy

Hch. Kündig & Cie. AG — Kündig Control Systems (KCS)

Geltungsbereich: Alle KCS-Produkte mit digitalen Elementen
Rechtsgrundlage: Verordnung (EU) 2024/2847 (Cyber Resilience Act), Art. 13 Abs. 6
Version: 1.1 | **Datum:** 2026-05-07

1. Einleitung

Die Hch. Kündig & Cie. AG nimmt die Sicherheit ihrer Produkte ernst. Ihre Fachabteilung Kündig Control Systems (KCS) begrüsst Meldungen von Sicherheitsforschern, Kunden und der Öffentlichkeit über potenzielle Schwachstellen in KCS-Produkten.

Diese CVD-Policy beschreibt, wie Schwachstellen an KCS gemeldet werden können, wie KCS damit umgeht und welche Erwartungen Meldende haben können.

2. Kontakt

Kanal	Adresse
E-Mail (bevorzugt)	security@gauge.ch
Betreff	[SECURITY] <Produktname> <Kurzbeschreibung>

Wir behandeln alle Meldungen vertraulich.

Reaktionszeit: KCS bestätigt den Eingang innerhalb von **5 Werktagen**.

3. Geltungsbereich

Diese Policy gilt für Schwachstellen in Produkten, welche von KCS vertrieben werden.

Nicht in Scope:

- Physische Sicherheit von KCS-Bürogebäuden
- Schwachstellen in Drittanbieter-Produkten, die nicht Teil eines KCS-Produkts sind
- Social Engineering gegen KCS-Mitarbeiter

4. Unsere Erwartungen an Meldende (Safe Harbour)

Hch. Kündig & Cie. AG / KCS verpflichtet sich, gegenüber Personen, die in gutem Glauben und gemäss dieser Policy handeln, **keine rechtlichen Schritte einzuleiten**, sofern folgende Regeln eingehalten werden:

Erlaubt:

- ✓ Schwachstellen in eigenen Systemen oder mit expliziter schriftlicher Genehmigung testen
- ✓ Gefundene Schwachstellen über security@gauge.ch melden
- ✓ Koordinierte Offenlegung nach Absprache mit KCS

Nicht erlaubt:

✗ Zugriff auf Kundendaten oder Produktionssysteme Dritter

✗ Destruktive Tests (DoS, Datenzerstörung)

✗ Öffentliche Offenlegung vor Ablauf der Koordinationsperiode

✗ Nutzung der Schwachstelle für eigene Zwecke

5. Prozess nach Eingang einer Meldung

Schritt	Frist	Beschreibung
Eingangsbestätigung	5 Werktage	KCS bestätigt Eingang und teilt eine Tracking-ID mit
Erstbeurteilung	10 Werktage	KCS bewertet Schweregrad und Reproduzierbarkeit
Statusupdate	30 Tage	KCS informiert Meldenden über Fortschritt
Behebung	Gemäss Severity	Critical 7d, High 30d, Medium 90d, Low 180d
Koordinierte Offenlegung	Nach Patch-Release	KCS informiert Meldenden; gemeinsame Offenlegung möglich

6. Was KCS von Meldenden erwartet

- **Koordination:** Keine öffentliche Offenlegung vor Ablauf der Koordinationsperiode (max. 90 Tage)
- **Minimalinvasiv:** Kein unnötiger Zugriff über das zur Verifikation nötige Mass hinaus
- **Dokumentation:** Ausreichende Informationen zur Reproduzierbarkeit der Schwachstelle
- **Kontakt:** Erreichbarkeit für Rückfragen während der Koordinationsperiode

7. Was Meldende von KCS erwarten können

- Schnelle Eingangsbestätigung
- Transparente Kommunikation über Bearbeitungsstand
- Anerkennung im Security Advisory (auf Wunsch, mit Einverständnis des Meldenden)
- Keine rechtlichen Schritte bei Einhaltung dieser Policy

8. Änderungshistorie

Version	Datum	Änderung
1.0	2026-04-13	Erstversion
1.1	2026-05-07	Separate DE/EN Dokumente

Verantwortlich: Roger Fässler, PSIRT-Leiter — Hch. Kündig & Cie. AG / Kündig Control Systems (KCS), security@gauge.ch