G. Kraft Maschinenbau GmbH

Coordinated Vulnerability Disclosure Policy

(CVD-Lite / Vulnerability Disclosure Policy)

Status: **Freigegeben / gültig ab 03.09.2026**

Version: 1.0

Datum: 03.09.2026

Klassifizierung: Öffentlich

Verantwortlich: Kraft-Group PSIRT

1. Einleitung / Geltungsbereich

G. Kraft Maschinenbau GmbH nimmt die Sicherheit ihrer Produkte ernst und arbeitet daran, gemeldete Schwachstellen zeitnah zu bewerten und zu beheben. Ziel dieser Policy ist es, Sicherheitsforschenden und anderen Meldenden klare Leitlinien an die Hand zu geben, wie Schwachstellen in unseren Produkten gemeldet werden können und wie wir mit solchen Meldungen umgehen.

Diese Policy beschreibt, welche Produkte davon umfasst sind, wie Meldungen an uns übermittelt werden können, und wie wir den Prozess von der Meldung bis zur Veröffentlichung gestalten.

Wir ermutigen ausdrücklich dazu, uns über entdeckte Schwachstellen in unseren Produkten zu informieren.

G. Kraft Maschinenbau GmbH betreibt ein Product Security Incident Response Team (PSIRT), das für die Entgegennahme, Bewertung und Koordination von Schwachstellenmeldungen zuständig ist.

Diese Policy gilt für:

- alle von G. Kraft Maschinenbau GmbH entwickelten Software-Produkte,
- die von G. Kraft Maschinenbau GmbH unter eigenem Namen in Verkehr gebrachten Anlagen als Gesamtprodukt, einschließlich darin integrierter elektronischer Komponenten Dritter.

Für Schwachstellen in zugekauften elektronischen Komponenten koordiniert das PSIRT die Meldung an den jeweiligen Komponentenhersteller. G. Kraft Maschinenbau GmbH bleibt als Inverkehrbringer der Anlage jedoch Ansprechpartner für Meldende.

2. Meldekanal

Zur Meldung einer Sicherheitslücke in einem Produkt von G. Kraft Maschinenbau GmbH stehen folgende Kontaktmöglichkeiten zur Verfügung:

- E-Mail: security@kraft-group.com
- Kontaktformular: https://www.kraft-group.com/service/psirt

Verschlüsselte Übermittlung

Zur vertraulichen Übermittlung sensibler Inhalte (z. B. Proof-of-Concept-Code, Exploit-Details) empfehlen wir die Verschlüsselung mittels PGP. Eine Verschlüsselung ist nicht zwingend erforderlich, wird jedoch ausdrücklich empfohlen.

- PGP-Key: abrufbar auf unserer PSIRT-Seite unter https://www.kraft-group.com/service/psirt
- Fingerprint: 36DF 3E7A 9202 EC92 958F B679 CC78 7E5D 3A39 4745
- Zugeordnete E-Mail-Adresse: security@kraft-group.com

Bitte überprüfen Sie den Fingerprint des heruntergeladenen Schlüssels vor der Verwendung.

Bitte stellen Sie uns in Ihrer Meldung die folgenden Informationen bereit:

- Name der meldenden Person
- Kontaktdetails: E-Mail-Adresse und Telefonnummer
- Name der Organisation
- Name der betroffenen Anlage
- Betroffene Komponente
- Soft- oder Firmware-Version
- Art der Schwachstelle (z. B. XSS, Pufferüberlauf, fest codierte Zugangsdaten, CWE-ID, CVE-ID falls verfügbar)
- Beschreibung der Schwachstelle, ggf. inkl. Proof-of-Concept oder Netzwerk-Traces
- Angabe, ob die Schwachstelle bereits öffentlich bekannt ist
- Einverständnis zur Nennung als Melder in einer möglichen Veröffentlichung (falls gewünscht)

Datei-Upload

Über unser Kontaktformular können ergänzend Dateien hochgeladen werden. Zulässig sind folgende Dateitypen:

Zweck	Zulässige Dateitypen
Beschreibung/Dokumentation	.pdf, .txt, .md
Screenshots/Bildbeweise	.png, .jpg, .jpeg
Netzwerk-Traces	.pcap, .pcapng
Log-Dateien	.log, .txt, .csv
PoC-Code / mehrere Dateien gebündelt	.zip
PGP-verschlüsselte/-signierte Dateien	.gpg, .pgp, .asc

Für sensible Inhalte empfehlen wir, die Datei vor dem Upload mit unserem PGP-Key zu verschlüsseln.

Eine Vorabinformation ohne NDA ist möglich; wir bitten jedoch um koordinierte Offenlegung, da eine sofortige öffentliche Veröffentlichung eine „0-Day-Situation“ schafft, die unsere Kunden unötig gefährdet.

Wir bestätigen den Eingang Ihrer Meldung so schnell wie möglich.

3. Umgang mit Kontaktdaten der Melder

Wenn G. Kraft Maschinenbau GmbH eine als ernsthaft eingestufte Schwachstellenmeldung erhält, werden die Kontaktdaten der meldenden Person, sofern noch nicht vorhanden, in unserer Melder-Datenbank erfasst. Die Verwaltung dieser Daten erfolgt im Einklang mit den Vorgaben der Datenschutz-Grundverordnung (DSGVO).

Die Kontaktdaten werden ausschließlich zur Kontaktaufnahme und Kommunikation im Rahmen der gemeldeten Schwachstelle verwendet. Auf ausdrücklichen Wunsch werden die Daten der meldenden

Person gelöscht. Auf ausdrücklichen Wunsch der meldenden Person kann sie zusätzlich namentlich in einer veröffentlichten Advisory als Melder genannt werden.

Weitere Informationen zum Umgang mit personenbezogenen Daten, einschließlich der Speicherdauer, finden Sie in unserer Datenschutzerklärung: https://www.kraft-group.com/datenschutz/

4. Analyse und Klassifizierung

G. Kraft Maschinenbau GmbH prüft und bewertet die Gültigkeit jeder eingegangenen Meldung. Relevanz und Auswirkung auf unsere Produkte werden verifiziert; bei Bedarf fordert das PSIRT weitere Informationen von der meldenden Person an.

Zur Einstufung der Schwachstelle verwendet G. Kraft Maschinenbau GmbH das Common Vulnerability Scoring System (CVSS) in der jeweils aktuellen Version. Der ermittelte CVSS-Score wird anhand folgender Skala in ein Security Impact Rating (SIR) übersetzt:

CVSS-Score	Security Impact Rating (SIR)
0,1 – 3,9	Low
4,0 – 6,9	Medium
7,0 – 8,9	High
9,0 – 10,0	Critical

Das PSIRT ist für die Berechnung des CVSS-Scores und die daraus resultierende Einstufung zuständig.

Für Schwachstellen in elektronischen Komponenten, die G. Kraft Maschinenbau GmbH nicht selbst entwickelt, sondern zukauft, übernimmt G. Kraft Maschinenbau GmbH grundsätzlich die vom Komponentenhersteller bereitgestellte Einstufung (SIR bzw. CVSS-Score). Eine solche Meldung wird durch das PSIRT intern nachverfolgt und an den zuständigen Komponentenhersteller koordiniert; eine eigene, unter dem Namen von G. Kraft Maschinenbau GmbH geführte Schwachstellen-Advisory erfolgt hierfür nicht, sofern die Schwachstelle eindeutig auf die Drittkomponente zurückzuführen ist.

5. Handling / Behebung

G. Kraft Maschinenbau GmbH führt die interne Bearbeitung gemeldeter Schwachstellen in Zusammenarbeit mit den zuständigen internen Entwicklungsteams durch. Während der Bearbeitung hält das PSIRT regelmäßigen Kontakt mit der meldenden Person, informiert über den aktuellen Stand und stellt sicher, dass unsere Position nachvollziehbar kommuniziert wird. Sofern verfügbar, können Vorab-Versionen von Fixes oder Advisories der meldenden Person zur Verifikation zur Verfügung gestellt werden.

Die Reaktionszeit bis zur Bereitstellung einer Behebung hängt von verschiedenen Faktoren ab, u. a. der Schwere der Schwachstelle, dem betroffenen Produkt, dem aktuellen Entwicklungszyklus sowie eventuellen Qualitätssicherungsmaßnahmen, und davon, ob die Behebung nur im Rahmen eines größeren Releases möglich ist.

Unbeschadet dessen garantiert G. Kraft Maschinenbau GmbH keine bestimmte Lösung für gemeldete Probleme; nicht jede identifizierte Schwachstelle kann behoben werden.

6. Disclosure / Veröffentlichung

G. Kraft Maschinenbau GmbH veröffentlicht Informationen zu behobenen Schwachstellen in Form einer Security Advisory. Dies gilt unabhängig von der Einstufung der Schwachstelle (Low, Medium, High, Critical). G. Kraft Maschinenbau GmbH behält sich vor, von dieser Vorgehensweise im Einzelfall abzuweichen, etwa wenn zusätzliche Faktoren nicht angemessen abgebildet werden können, und in solchen Fällen ggf. keine Advisory zu veröffentlichen.

Security Advisories werden auf unserer PSIRT-Seite veröffentlicht: https://www.kraft-group.com/service/psirt

Eine Security Advisory enthält üblicherweise folgende Informationen:

- Beschreibung der Schwachstelle mit CVE-Referenz (falls vorhanden) und CVSS-Score
- Betroffene Produkte sowie Software-/Firmware-Versionen
- Hinweise zu mildernden Faktoren und Workarounds
- Art und Verfügbarkeit der Behebung
- Mit Einverständnis der meldenden Person: Nennung als Melder für die Meldung und Zusammenarbeit

7. CVE-Vergabe

G. Kraft Maschinenbau GmbH beantragt nicht standardmäßig eine CVE-Nummer für Schwachstellen in eigener Software. Auf ausdrücklichen Wunsch der meldenden Person oder aus sonstigen Koordinationsgründen kann G. Kraft Maschinenbau GmbH im Einzelfall eine CVE-Nummer bei einer zuständigen CVE-Vergabestelle (CVE Numbering Authority, CNA) beantragen.

G. Kraft Maschinenbau GmbH prüft im Bedarfsfall, über welche CVE-Vergabestelle (CNA) eine CVE-Nummer beantragt werden kann, u. a. CERT@VDE (seit 2025 Root-CNA für die Automatisierungsindustrie in Deutschland) oder ersatzweise MITRE als global zuständige CNA of Last Resort.

Für Schwachstellen in zugekauften elektronischen Komponenten Dritter erfolgt die CVE-Vergabe in der Regel durch den jeweiligen Komponentenhersteller bzw. dessen zuständige CNA.

Hinweis: G. Kraft Maschinenbau GmbH vergibt bzw. beantragt keine CVE-Kennung für gemeldete Schwachstellen, bevor diese von G. Kraft Maschinenbau GmbH bestätigt wurden oder sich in einer verwendeten Drittkomponente befinden.

8. Kundenbenachrichtigung

G. Kraft Maschinenbau GmbH veröffentlicht Informationen zu Schwachstellen und verfügbaren Behebungen auf der PSIRT-Seite: https://www.kraft-group.com/service/psirt. Eine darüberhinausgehende individuelle Benachrichtigung einzelner Kunden wird nicht zugesichert.

Sofern unser PSIRT beobachtet, dass eine Schwachstelle aktiv ausgenutzt wird und dies zu einem erhöhten Risiko für unsere Kunden führen könnte, beschleunigt G. Kraft Maschinenbau GmbH die Veröffentlichung einer entsprechenden Sicherheitsmitteilung – auch wenn diese noch keinen vollständigen Fix oder Workaround enthält.

9. Meldepflicht bei aktiver Ausnutzung (Art. 14 CRA)

Über die in dieser Policy beschriebene Zusammenarbeit mit meldenden Personen hinaus unterliegt G. Kraft Maschinenbau GmbH als Hersteller von Produkten mit digitalen Elementen den gesetzlichen Meldepflichten nach Art. 14 der Verordnung (EU) 2024/2847 (Cyber Resilience Act, CRA).

Wird eine Schwachstelle in einem Produkt von G. Kraft Maschinenbau GmbH aktiv ausgenutzt, oder liegt ein schwerwiegender Sicherheitsvorfall vor, der die Sicherheit unserer Produkte beeinträchtigt, meldet unser PSIRT dies fristgerecht über die einheitliche Meldeplattform (Single Reporting Platform) der ENISA an das zuständige Computer Security Incident Response Team (CSIRT). Nach aktuellem Stand (August 2026) ist hierfür in Deutschland das beim BSI angesiedelte CSIRT vorgesehen.

G. Kraft Maschinenbau GmbH kommt dabei den gesetzlich vorgeschriebenen Fristen für Frühwarnung, Meldung und Abschlussbericht gemäß Art. 14 CRA nach. Die Information betroffener Nutzer erfolgt im Rahmen der in Kapitel 8 beschriebenen Kommunikationswege.

10. Definitionen

PSIRT: Ein Team, das für die Bearbeitung von Sicherheitsproblemen in einem Produkt oder einer Dienstleistung zuständig ist. Je nach Ausgestaltung kann dies ein formelles Sicherheitsteam einer Organisation, eine Gruppe von Freiwilligen in einem Open-Source-Projekt oder ein unabhängiges Gremium sein.

Melder (meldende Person): Jede Person, die eine potenzielle Sicherheitslücke in irgendeiner Form von Technologie untersucht hat, einschließlich akademischer Sicherheitsforschender, Softwareentwicklerinnen und -entwickler, Systemadministratorinnen und -administratoren sowie technisch interessierter Privatpersonen.

Report (Meldung): Die Beschreibung einer potenziellen Sicherheitslücke in einem bestimmten Produkt oder einer Dienstleistung durch einen Melder. Meldungen beginnen stets als nicht-öffentliche Übermittlung an das PSIRT von G. Kraft Maschinenbau GmbH.

Schwachstelle (Vulnerability): Ein Fehler in Software oder Firmware, der es einem Angreifer ermöglichen würde, eine Handlung entgegen einer festgelegten Sicherheitsrichtlinie durchzuführen. Ein Fehler, der einen erweiterten Zugriff oder erweiterte Rechte ermöglicht, ist eine Schwachstelle.

Auch Designfehler und Verstöße gegen anerkannte Sicherheitsgrundsätze können als Schwachstellen gelten.

CVE (Common Vulnerabilities and Exposures): Ein Verzeichnis, das Definitionen für öffentlich bekannt gemachte Cybersicherheits-Schwachstellen bereitstellt, um den Datenaustausch zwischen verschiedenen Sicherheitswerkzeugen, Datenbanken und Diensten zu erleichtern. Ein CVE-Eintrag besteht aus einer Kennung, einer Beschreibung und mindestens einer öffentlichen Referenz.

CNA (CVE Numbering Authority): Eine von der CVE-Organisation autorisierte Stelle, die berechtigt ist, CVE-Kennungen zu vergeben.

CVSS (Common Vulnerability Scoring System): Ein standardisiertes Bewertungssystem zur Einschätzung des Schweregrads von Sicherheitslücken anhand eines numerischen Scores (0,0 bis 10,0).

SIR (Security Impact Rating): Die interne qualitative Einstufung einer Schwachstelle durch G. Kraft Maschinenbau GmbH (Low, Medium, High, Critical) auf Basis des CVSS-Scores (siehe Kapitel 4).

CRA (Cyber Resilience Act): Die Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen.

CSIRT (Computer Security Incident Response Team): Eine staatlich benannte Stelle zur Entgegennahme von Meldungen über Schwachstellen und Sicherheitsvorfälle im Rahmen des CRA; in Deutschland nach aktuellem Stand das beim BSI angesiedelte CSIRT.

11. Versionshistorie

Version	Datum	Änderungen gegenüber der letzten Version
1.0	03.09.2026	Erstveröffentlichung

Ersteller/Verantwortlich: Kraft-Group PSIRT