G. Kraft Maschinenbau GmbH

Coordinated Vulnerability Disclosure Policy

(CVD-Lite / Vulnerability Disclosure Policy)

Status: **Released / effective from 03.09.2026**

Version: 1.0

Date: 03.09.2026

Classification: Public

Responsible: Kraft-Group PSIRT

1. Introduction / Scope

G. Kraft Maschinenbau GmbH takes the security of its products seriously and works to promptly assess and remediate reported vulnerabilities. The purpose of this policy is to give security researchers and other reporters clear guidance on how to report vulnerabilities in our products and how we handle such reports.

This policy describes which products are covered, how reports can be submitted to us, and how we shape the process from report to publication.

We explicitly encourage you to inform us about vulnerabilities discovered in our products.

G. Kraft Maschinenbau GmbH operates a Product Security Incident Response Team (PSIRT), which is responsible for receiving, assessing, and coordinating vulnerability reports.

This policy applies to:

- all software products developed by G. Kraft Maschinenbau GmbH,
- the systems placed on the market by G. Kraft Maschinenbau GmbH under its own name as a complete product, including third-party electronic components integrated therein.

For vulnerabilities in purchased electronic components, the PSIRT coordinates the report with the respective component manufacturer. However, G. Kraft Maschinenbau GmbH remains the point of contact for reporters as the party placing the system on the market.

2. Reporting Channel

The following contact options are available for reporting a security vulnerability in a product of G. Kraft Maschinenbau GmbH:

- Email: security@kraft-group.com
- Contact form: https://www.kraft-group.com/service/psirt

Encrypted Submission

For the confidential submission of sensitive content (e.g. proof-of-concept code, exploit details), we recommend encryption using PGP. Encryption is not mandatory but is explicitly recommended.

- PGP key: available on our PSIRT page at https://www.kraft-group.com/service/psirt
- Fingerprint: 36DF 3E7A 9202 EC92 958F B679 CC78 7E5D 3A39 4745
- Associated email address: security@kraft-group.com

Please verify the fingerprint of the downloaded key before use.

Please provide us with the following information in your report:

- Name of the reporting person
- Contact details: email address and phone number

- Name of the organization
- Name of the affected system
- Affected component
- Software or firmware version
- Type of vulnerability (e.g. XSS, buffer overflow, hard-coded credentials, CWE ID, CVE ID if available)
- Description of the vulnerability, including proof-of-concept or network traces if available
- Indication of whether the vulnerability has already been publicly disclosed
- Consent to being credited as the reporter in a possible publication (if desired)

File Upload

Files can also be uploaded via our contact form. The following file types are permitted:

Purpose	Permitted file types
Description/documentation	.pdf, .txt, .md
Screenshots/visual evidence	.png, .jpg, .jpeg
Network traces	.pcap, .pcapng
Log files	.log, .txt, .csv
PoC code / multiple bundled files	.zip
PGP-encrypted/-signed files	.gpg, .pgp, .asc

For sensitive content, we recommend encrypting the file with our PGP key before uploading.

Advance notice without an NDA is possible; however, we ask for coordinated disclosure, as immediate public disclosure creates a „0-day situation“ that unnecessarily endangers our customers.

We will confirm receipt of your report as soon as possible.

3. Handling of Reporters' Contact Data

If G. Kraft Maschinenbau GmbH receives a vulnerability report classified as serious, the contact details of the reporting person, if not already available, are recorded in our reporter database. This data is managed in accordance with the requirements of the General Data Protection Regulation (GDPR).

The contact details are used exclusively for contacting and communicating with the reporter in connection with the reported vulnerability. Upon explicit request, the reporting person's data will be deleted. At the explicit request of the reporting person, they may also be credited by name as the reporter in a published advisory.

For further information on the handling of personal data, including the retention period, please refer to our privacy policy: https://www.kraft-group.com/datenschutz/

4. Analysis and Classification

G. Kraft Maschinenbau GmbH reviews and assesses the validity of each report received. Relevance and impact on our products are verified; if necessary, the PSIRT will request additional information from the reporting person.

To classify a vulnerability, G. Kraft Maschinenbau GmbH uses the Common Vulnerability Scoring System (CVSS) in its current version. The resulting CVSS score is translated into a Security Impact Rating (SIR) according to the following scale:

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

The PSIRT is responsible for calculating the CVSS score and the resulting classification.

For vulnerabilities in electronic components that G. Kraft Maschinenbau GmbH does not develop itself but purchases, G. Kraft Maschinenbau GmbH generally adopts the classification (SIR or CVSS score) provided by the component manufacturer. Such a report is tracked internally by the PSIRT and coordinated with the responsible component manufacturer; G. Kraft Maschinenbau GmbH will not issue its own vulnerability advisory under its own name in such cases, provided the vulnerability is clearly attributable to the third-party component.

5. Handling / Remediation

G. Kraft Maschinenbau GmbH handles the internal processing of reported vulnerabilities in cooperation with the responsible internal development teams. During processing, the PSIRT maintains regular contact with the reporting person, provides updates on the current status, and ensures that our position is communicated in a comprehensible manner. Where available, preliminary versions of fixes or advisories may be provided to the reporting person for verification.

The response time until a remediation is provided depends on various factors, including the severity of the vulnerability, the affected product, the current development cycle, any quality assurance measures, and whether the remediation is only possible as part of a larger release.

Notwithstanding the foregoing, G. Kraft Maschinenbau GmbH does not guarantee a specific resolution for reported issues; not every identified vulnerability can be remediated.

6. Disclosure / Publication

G. Kraft Maschinenbau GmbH publishes information on remediated vulnerabilities in the form of a security advisory. This applies regardless of the vulnerability's classification (Low, Medium, High,

Critical). G. Kraft Maschinenbau GmbH reserves the right to deviate from this approach on a case-by-case basis, for example if additional factors cannot be adequately reflected, and in such cases may decide not to publish an advisory.

Security advisories are published on our PSIRT page: https://www.kraft-group.com/service/psirt

A security advisory usually contains the following information:

- Description of the vulnerability with CVE reference (if available) and CVSS score
- Affected products and software/firmware versions
- Information on mitigating factors and workarounds
- Type and availability of the remediation
- With the consent of the reporting person: credit as reporter for the report and cooperation

7. CVE Assignment

G. Kraft Maschinenbau GmbH does not request a CVE number as a standard practice for vulnerabilities in its own software. At the explicit request of the reporting person or for other coordination reasons, G. Kraft Maschinenbau GmbH may, on a case-by-case basis, request a CVE number from a responsible CVE Numbering Authority (CNA).

If needed, G. Kraft Maschinenbau GmbH will determine which CVE Numbering Authority (CNA) to approach, including CERT@VDE (Root CNA for the automation industry in Germany since 2025) or, alternatively, MITRE as the globally responsible CNA of Last Resort.

For vulnerabilities in purchased third-party electronic components, the CVE is generally assigned by the respective component manufacturer or its responsible CNA.

Note: G. Kraft Maschinenbau GmbH does not assign or request a CVE identifier for reported vulnerabilities until they have been confirmed by G. Kraft Maschinenbau GmbH or are found to reside in a used third-party component.

8. Customer Notification

G. Kraft Maschinenbau GmbH publishes information on vulnerabilities and available remediations on the PSIRT page: https://www.kraft-group.com/service/psirt. Any additional individual notification of specific customers is not guaranteed.

If our PSIRT observes that a vulnerability is being actively exploited and this could lead to increased risk for our customers, G. Kraft Maschinenbau GmbH will expedite the publication of a corresponding security notice – even if it does not yet include a complete fix or workaround.

9. Reporting Obligation in the Event of Active Exploitation (Art. 14 CRA)

In addition to the cooperation with reporting persons described in this policy, G. Kraft Maschinenbau GmbH, as a manufacturer of products with digital elements, is subject to the statutory reporting obligations under Article 14 of Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA).

If a vulnerability in a product of G. Kraft Maschinenbau GmbH is actively exploited, or if a serious security incident occurs that affects the security of our products, our PSIRT will report this within the applicable deadlines via ENISA's Single Reporting Platform to the responsible Computer Security Incident Response Team (CSIRT). As of the current status (August 2026), the CSIRT located at the BSI is designated for this purpose in Germany.

G. Kraft Maschinenbau GmbH complies with the statutory deadlines for the early warning, notification, and final report pursuant to Art. 14 CRA. Affected users are informed through the communication channels described in Chapter 8.

10. Definitions

PSIRT: A team responsible for addressing security issues in a product or service. Depending on the setup, this may be a formal security team within an organization, a group of volunteers on an open-source project, or an independent panel.

Reporter (reporting person): Any person who has investigated a potential security vulnerability in any form of technology, including academic security researchers, software developers, system administrators, and technically interested private individuals.

Report: A reporter's description of a potential security vulnerability in a specific product or service. Reports always begin as non-public submissions to the PSIRT of G. Kraft Maschinenbau GmbH.

Vulnerability: A flaw in software or firmware that would allow an attacker to perform an action in violation of a defined security policy. A flaw that enables elevated access or privileges is a vulnerability. Design flaws and violations of recognized security principles may also qualify as vulnerabilities.

CVE (Common Vulnerabilities and Exposures): A dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities, in order to facilitate data exchange between different security tools, databases, and services. A CVE entry consists of an identifier, a description, and at least one public reference.

CNA (CVE Numbering Authority): An organization authorized by the CVE Program to assign CVE identifiers.

CVSS (Common Vulnerability Scoring System): A standardized rating system for assessing the severity of vulnerabilities based on a numerical score (0.0 to 10.0).

SIR (Security Impact Rating): The internal qualitative classification of a vulnerability by G. Kraft Maschinenbau GmbH (Low, Medium, High, Critical) based on the CVSS score (see Chapter 4).

CRA (Cyber Resilience Act): Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements.

CSIRT (Computer Security Incident Response Team): A government-designated body for receiving reports on vulnerabilities and security incidents under the CRA; in Germany, currently the CSIRT located at the BSI.

11. Version History

Version	Date	Changes compared to the previous version
1.0	03.09.2026	Initial publication

Author/Responsible: Kraft-Group PSIRT