# Coordinated Vulnerability Disclosure Policy

## Introduction

This document describes all relevant information about the CVD process at Kendrion Kuhnke Automation GmbH (KENDRION).
KENDRION products and services are subject to the highest quality requirements. Cyber security is therefore also considered and tested during development. To ensure that this is maintained throughout the entire service life of the products and services, reports of potential vulnerabilities are taken very seriously and handled responsibly. The detection of vulnerabilities is seen as a joint effort by a wide range of parties with the aim of offering our customers a consistently high level of security.

Product security is of utmost importance to KENDRION. We are therefore highly committed to resolving vulnerabilities and to supporting the security and safety of KENDRION industrial control systems. KENDRION strongly recommends coordinated vulnerability disclosure. Only then do we have the opportunity to fix a flaw before it is publicly disclosed. Our aim is to provide our customers with high-quality security updates and to prevent them from being exposed to malicious attacks while the update is being developed. This document describes how to report potential security vulnerabilities affecting the KENDRION products to KENDRION and how customers are informed by KENDRION about verified vulnerabilities, resolutions and mitigations.

## CERT@VDE

As the first IT security platform to support small and medium-sized enterprises (SMEs) in the automation industry with IT security issues,-CERT@VDE enables an open professional exchange on security standards and risks. KENDRION is one of the cooperation partners and provides information on the platform about security-related incidents or potential vulnerabilities. CERT@VDE thus offers a central platform through which previously isolated information is bundled, structured, and distributed. Kendrion publishes vulnerabilities via CERT@VDE and receives them via CERT@VDE. Customers are provided with information on security-related incidents, such as vulnerabilities in their own products or cyber-attacks, via this central point of contact. In this way, KENDRION makes a significant contribution to improving cyber security in the operation of KENDRION products.

## Reporting of vulnerabilities

KENDRION strongly encourages the reporting of possible vulnerabilities or other security issues. We ask anyone who discovers a vulnerability affecting the KENDRION products to report it directly to us or to CERT@VDE. As mentioned above, an immediate public disclosure may encourage a malicious attack and cause serious security risks for control systems, machines, plants or other devices operated with KENDRION products. All vulnerability reports are handled with utmost care and the interests of the reporting party are respected and observed.
Discovered vulnerabilities should be reported per email to the KENDRION Security Team at **psirt@KENDRION.com** or to CERT@VDE at **info@cert.vde.com**.

When reporting a vulnerability or other security issues please include the following information:

- Name and version of the affected product
- A simple description (if necessary screenshots or other illustrations for better comprehensibility) showing how the vulnerability was discovered (including any tools used).
- Publicity of vulnerability

If possible, a vulnerability report should also contain the following further information:

- An assignment of the vulnerability to the OWASP Top 10 2021 (see https://owasp.org/www-project-top-ten). If none of the vulnerability categories fit, this should be described in more detail as "Other"
- Proof-of-concept (PoC) code or instructions showing how the vulnerability can be exploited.
- A risk assessment, taking into account the technical conditions to determine the severity of the vulnerability (e.g. by using a CVSS value and the associated matrix -- preferably in the most current version).
- A description of the impact of the reported vulnerability or a threat model that describes a relevant attack scenario.

Reporting parties who provide their email address will receive a prompt acknowledgement of receipt and will be contacted for follow-up.

## PGP encryption

You've found a vulnerability in one of our partner's products? Don't hesitate to contact us via Email (with optional PGP encryption). Encrypted messages are preferred to protect sensitive information and data. The languages accepted are German and English.

**Email** info@cert.vde.com
**PGP-Key** 4096R/C3E3E8AD download
**PGP-Fingerprint** F5F7 FFB6 32D9 EAC7 1E74 F344 0CF5 E79A C3E3 E8AD

**Email** psirt@kendrion.com
**PGP-Schlüssel ID** 642D 4313 download
**PGP-Fingerabdruck** 214E A7EB 7CA2 26A3 F98E 6598 DE87 EDF4 642D 4313

## Internal vulnerability handling

All security vulnerabilities reported to KENDRION are thoroughly investigated, assessed and prioritized. Goal is to identify all possibly affected products, determine the root cause of the vulnerability, and develop a resolution or remediation. KENDRION may possibly request more information from the reporter in this process.
KENDRION may inform official CERTs via CERT@VDE and interested OEMs and maintain active communication with these and the reporting party to inform about remediation and software updates. If available, pre-releases of software or firmware fixes can be provided to the reporter for verification.

## Advisory

Once a mitigation or resolution (usually software/firmware update) is available, KENDRION will release an advisory.
This advisory is published on the CERT@VDE website under
https://certvde.com/de/advisories/vendor/KENDRION/
An advisory usually contains the following:

- Description of the vulnerability and its severity (based on CVSS score)
- Identification of products and versions affected
- Information on mitigating factors and workarounds
- Timeline and availability of software security updates
- With the reporting party’s consent, credit is provided for reporting and collaboration

Information about our CSAF Advisories can be found at
**https://kendrion.csaf-tp.certvde.com/.well-known/csaf/provider-metadata.json**

## Customized Solutions

In some cases, disclosure may be limited to one or a specific group of customers. These customers are contacted directly and the advisory in question is published for them only. As each security vulnerability case is different, we may take alternative actions if necessary.

## Contact information

Website: www.KENDRION.com
Email: psirt@KENDRION.com

## Disclaimer



**Change History**

| Version | Description | Date |
|---|---|---|
| 1.0 | First version | 27.02.2025 |
| 1.01 | PGP encryption | 10.04.2025 |