Security Vulnerability Disclosure Policy

Version: 1.0 Release date: 10 September 2026

Introduction

koenig-pa develops software products for industrial EtherCAT applications. We are committed to the security of these products and to the security of our customers' production environments.

This policy defines how security researchers, customers, and the general public can report potential security vulnerabilities to us, and how we handle and disclose such reports in a coordinated manner. We follow the principles of ISO/IEC 29147 (Coordinated Vulnerability Disclosure, CVD) and comply with the applicable obligations under the EU Cyber Resilience Act (Regulation (EU) 2024/2847), in particular Article 14 concerning the reporting of actively exploited vulnerabilities and severe incidents.

Scope

This policy applies to all KPA products made available on the market, including: KPA EtherCAT Master, KPA EtherCAT Studio, KPA Motion Control Library, and KPA EtherCAT Slave Stack.

We accept vulnerability reports concerning all KPA products. The availability of security updates and mitigations depends on the applicable product support period and product lifecycle status.

Out of Scope

- Social engineering attacks
- Vulnerabilities in third-party products or components that do not affect a KPA product or its components.
- Physical security issues

How to Report

Please report security vulnerabilities by email: security@koenig-pa.de

If you prefer encrypted communication, you may encrypt your report using our PGP public key:

PGP Fingerprint: 47A3AC23C3CE69848A4271EDE6E614A908589DED

Public key download: https://koenig-pa.de/security/pgp.asc (also published on keys.openpgp.org)

If you cannot use email, you may use the HTTPS reporting form: https://koenig-pa.de/security/report-a-vulnerability/

Reports may be submitted at any time. Please do not use public channels (forums, social media) to report active vulnerabilities before we have had a reasonable opportunity to investigate the issue and coordinate disclosure.

Information to Include

To help us triage and investigate issues efficiently, please include as much of the following as possible:

- Product and exact version (e.g. "EtherCAT Master v2.8.2503.0") and affected component.
- Type of vulnerability, e.g. memory corruption, privilege escalation, improper authentication, denial of service, or unsafe network processing.

- Any assigned CVE ID (Common Vulnerabilities and Exposures), if applicable.
- A description of the vulnerability and its potential impact (e.g. remote code execution, privilege escalation, denial of service, data leakage).
- Steps to reproduce or a proof of concept (PoC), preferably minimal.
- Affected configurations and dependencies (e.g. OS, CPU architecture, EtherCAT network topology).
- Suggested mitigation or fix, if you have one.
- Your contact details and whether you wish to be publicly acknowledged.

If you encrypt your report with PGP, please also provide a brief unencrypted summary so that we can confirm receipt. Do not include sensitive vulnerability details in the unencrypted subject line or summary.

Rules of Engagement

We are grateful for research conducted in good faith. Please:

- Test only on your own systems or on test environments you are authorized to use.
- Do not perform attacks that could affect other users' systems or production machines.
- Do not attempt social engineering, physical attacks, or attacks against koenig-pa infrastructure.
- Do not exfiltrate, delete, or modify customer data beyond what is necessary to demonstrate the vulnerability.
- Do not publicly disclose the vulnerability before the end of the coordinated disclosure period (see Coordinated Disclosure Timeline).

Our Handling Process

Once we receive a report, we follow this process:

Stage	Timeline
Acknowledgement - we confirm receipt of your report	normally within 3 business days of receipt
Triage - initial assessment, severity, and first response	normally within 5 business days of receipt
Investigation and fix - development of a security update	as soon as possible, depending on severity
Coordinated disclosure	see Coordinated Disclosure Timeline

Severity is assessed based on the Common Vulnerability Scoring System (CVSS) and on the actual risk to industrial control environments. We may contact you during the investigation for additional details. Where applicable, we will fulfil the reporting and user notification obligations established by Article 14 of the EU Cyber Resilience Act within the required timeframes.

Coordinated Disclosure Timeline

As a general guideline, we aim to coordinate disclosure within 90 days of receiving a report. The actual timeline may be adjusted depending on the severity of the vulnerability, the availability of a fix or mitigation, the risk to affected users, and applicable legal requirements. We will coordinate the disclosure timeline with the reporter where reasonably possible.

Upon publication, we will:

- Credit you (if you agreed to be acknowledged).

- Publish the relevant security advisory and coordinate the assignment of a CVE ID, where appropriate.

Where required, we will inform affected users without undue delay and provide available mitigation or corrective measures.

Safe Harbor

If we determine that your research was conducted in good faith and in accordance with this policy, we do not intend to initiate legal action solely on the basis of that research.

This safe harbor applies only to research concerning KPA products and conducted in accordance with the Rules of Engagement set out above. We request that you make a good-faith effort to avoid privacy violations, service disruption, and destruction of data during your research.

Confidentiality and Data Handling

We treat all reports as confidential. We will:

- Handle your identity and report confidentially and disclose them only with your consent or where reasonably necessary to investigate or remediate the vulnerability, protect affected users, or comply with applicable law.
- Publish only the information necessary to describe and remediate the vulnerability.

We store reports and related data in accordance with applicable data protection law.

Acknowledgements

If you wish to be publicly credited, we will add your name (or alias) to our Security Acknowledgements page: https://koenig-pa.de/security/security-acknowledgements/.
If you prefer to remain anonymous, we fully respect that.

Our Security Response

Security advisories, security update information, and product support periods are published at: https://koenig-pa.de/security/security-advisories/.

For Software Bill of Materials (SBOM) requests, please contact: security@koenig-pa.de.

Changes to This Policy

This policy may be updated from time to time. Significant changes will be announced on our website. The latest version is always available at https://koenig-pa.de/security/vulnerability-disclosure-policy.

Security Contact

We publish a security.txt file at https://koenig-pa.de/.well-known/security.txt so that automated tools and researchers can discover our security contact information.

koenig-pa GmbH
Im Talesgrund 9a
91207 Lauf a.d. Pegnitz
Germany
https://koenig-pa.de/

Contact
email: sales@koenig-pa.de
tel.: +49 9128 725 330
tel.: +49 9123 960 5796