Guidance on Handling Security Vulnerabilities

Vulnerability Handling Guideline

The secure and responsible handling of security vulnerabilities is a key component of our product- s and information security. This guideline describes the fundamental principles, responsibilities and processes that ensure vulnerabilities in our products, systems and OT and IT environments are handled quickly, in a structured manner and in compliance with the law.
It serves as a guide for all employees and forms the basis for our PSIRT processes, coordinated vulnerability disclosure (CVD) and compliance with the reporting obligations under the Cyber Resilience Act (CRA).

1. Fundamental Principles

Our approach to security vulnerabilities follows five key guidelines:
Speed: Security vulnerabilities are assessed and addressed without delay to minimise risks at an early stage.
Transparency All steps – from reporting to resolution – are documented in a traceable manner.
Security: All measures are designed to protect our systems, products and customers.
Accountability: Anyone who identifies a vulnerability must report it immediately via the designated channels.
Compliance: We comply with all legal requirements, in particular the CRA and relevant ISO standards.

Reporting channels

Security vulnerabilities must only be reported via defined channels:

PSIRT email: psirt@trsystems.de
Internal ticketing system: OTOBO (ticket ID)
Direct report to PSIRT contact

External security researchers should use the CVD contact address and the published PGP (Pretty Good Privacy) key for encrypted communication.

Once a report has been submitted, the classification process begins. Each report is classified into one of the following categories:

- Vulnerability
- Security incident
- Change request

Vulnerabilities and incidents are prioritised and assessed by the PSIRT. The assessment is based on the following criteria

- Exploitability (CVSS)

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telephone: +49 (0) 7425 / 228 - 0, Fax: +49 (0) 7425 / 228 – 34, Email: sales@trsystems.de

Date: 01.07.2026

- Severity
- Affected products
- Evidence of active exploitation
- CRA relevance (reporting obligation)

The initial assessment is carried out within 24 hours of receipt of the report. In addition, an action plan is drawn up for each confirmed vulnerability.
This includes:

- Immediate measures
- Technical remediation
- Validation
- Documentation updates
- Communication measures

The action plan ensures that the vulnerability is rectified in a structured, comprehensive and traceable manner.
Communication is carried out depending on the severity and exploitation status:

- Internal notification to relevant departments
- Customer notification (e.g. PCN)
- Publication of a security advisory
- Reporting to ENISA or BSI if the vulnerability is being actively exploited
- Coordination with external security researchers (CVD)

Transparent communication is an essential part of secure vulnerability management.
Once all measures have been implemented, the following takes place:

- Final assessment by the PSIRT
- Full documentation in the ticket system
- Conducting a lessons learnt review and
- derivation of process improvements

This ensures that we not only rectify vulnerabilities but also continuously improve our processes.

Responsibilities: who does what?

PSIRT: Assessment, coordination, approval and communication
Line departments: analysis, technical implementation and testing
Stakeholders: Reporting vulnerabilities
Management: Provision of resources and approvals

Our approach is guided by the following standards and legal requirements:

- Cyber Resilience Act (CRA)
- ISO/IEC 30111 – Vulnerability Handling
- ISO/IEC 29147 – Vulnerability Disclosure
- ISO/IEC 27001 – Information Security
- Internal PSIRT processes and guidelines

This guide provides clear guidance on how security vulnerabilities are identified, assessed, handled and communicated within our organisation.
It creates transparency, strengthens the security of our products and ensures that we meet all legal requirements.

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telephone: +49 (0) 7425 / 228 - 0, Fax: +49 (0) 7425 / 228 – 34, Email: sales@trsystems.de