Richtlinie zur koordinierten Offenlegung von Sicherheitslücken

See English version below.

1. Einleitung

Diese Richtlinie zur koordinierten Offenlegung von Sicherheitslücken beschreibt den Prozess zur Meldung von potenziellen Sicherheitslücken in Produkten, Systemen oder Dienstleistungen von TROESTER und deren Tochterunternehmen.

Personen, die eine mögliche Schwachstelle identifizieren, können diese über die in dieser Richtlinie beschriebenen Meldewege an uns übermitteln. Ziel ist es, gemeldete Sachverhalte zu prüfen, deren Auswirkungen zu bewerten und gegebenenfalls geeignete Maßnahmen einzuleiten. Eine koordinierte Offenlegung soll dabei dazu beitragen, dass Informationen über Schwachstellen in geordneter Weise behandelt werden und betroffene Parteien ausreichend Gelegenheit erhalten, angemessene Maßnahmen umzusetzen.

Diese Richtlinie legt die Rahmenbedingungen für die Meldung, Bearbeitung und Kommunikation von Schwachstellenmeldungen fest und dient als Orientierung für alle beteiligten Parteien.

2. Meldung von Schwachstellen

Sollten Sie eine Sicherheitslücke in einem unserer Produkte oder Services identifizieren, melden Sie uns diese bitte per E-Mail an:

security@troester.de

Bitte liefern Sie uns im Rahmen Ihrer Meldung die folgenden Informationen:

- **Name des Melders:** (Falls Sie anonym bleiben möchten, respektieren wir Ihren Wunsch natürlich).
    - Ansonsten: E-Mail-Adresse und Telefonnummer, unter der wir Sie erreichen können.
    - Zugehörigkeit: Wie lautet Ihre Organisationszugehörigkeit (falls vorhanden)?

- **Art der eingereichten Sicherheitslücke:** Wie beschreiben Sie die Art der Sicherheitslücke (z. B. XSS, Pufferüberlauf, fest codierte Zugangsdaten …)?

- **Kurze Erläuterung der Schwachstelle** (ohne technische Details) und wie Sie die Schwachstelle gefunden haben

- **Betroffene Komponenten:** In welchen Produkten, Lösungen oder Diensten haben Sie die Sicherheitslücke gefunden? Fügen Sie alle Informationen ein, die Ihnen zur Verfügung stehen, wie Produktfamilie und -gruppe, Firmware- oder Software-Version. Geben Sie bei Diensten den jeweiligen Ort (z. B. URL) an.

- **Auslöser der Sicherheitslücke:** Können Sie Code bereitstellen, mit dem das Auslösen der Sicherheitslücke nachgewiesen werden kann (Proof-of-Concept, PoC)? Als Alternative können Sie auch Network-Traces (z. B. pcaps) oder eine Beschreibung zur Reproduktion der Sicherheitslücke einreichen.

- **Auswirkungen der Sicherheitslücke:** Haben Sie Auswirkungen beobachtet, die durch die Sicherheitslücke entstehen bzw. herbeigeführt werden?

- **Vertraulichkeit von Sicherheitslücken:** Wurde die Sicherheitslücke bereits offengelegt oder haben Sie konkrete Pläne für die Offenlegung?

Jedes Design- oder Implementierungsproblem kann gemeldet werden, wenn dies reproduzierbar ist und die Informations-, Produkt- oder IT-Sicherheit betrifft.

Bitte beachten Sie, dass die folgenden Schwachstellen nicht in den Anwendungsbereich dieser Richtlinie fallen:

- Angriffe, die einen physischen Zugriff auf das Gerät oder Netzwerk eines Benutzers erfordern
- Berichte von automatischen Tools oder Scans ohne erklärende Dokumentation
- Nicht umgesetzte Best Practices des Betreibers

3. TROESTER Versprechen

- Sie erhalten von uns innerhalb von 3 Werktagen (bezogen auf Deutschland, Hannover) eine Rückmeldung über den Eingang Ihrer Meldung.
  Weiterhin informieren wie Sie fortlaufend über die relevanten Schritte im Rahmen der Bearbeitung.

- Wir werden gemeldete Schwachstellen analysieren und bewerten, geeignete Maßnahmen zur Behebung entwickeln und diese in koordinierter Form kommunizieren.

- Wir werden Ihre Meldung vertraulich behandeln und Ihre persönlichen Daten nicht ohne Ihre Zustimmung an Dritte weitergeben.

Policy on Coordinated Vulnerability Disclosure

1. Introduction

This Policy on the Coordinated Disclosure of Security Vulnerabilities describes the process for reporting potential security vulnerabilities in products, systems, or services provided by TROESTER and its subsidiaries.

Individuals who identify a potential vulnerability may report it to us via the reporting channels described in this policy. The goal is to investigate reported issues, assess their impact, and, if necessary, take appropriate action. Coordinated disclosure is intended to ensure that information about vulnerabilities is handled in an orderly manner and that affected parties are given sufficient opportunity to implement appropriate measures.

This policy establishes the framework for the reporting, handling, and communication of vulnerability reports and serves as a guide for all parties involved.

2. Reporting Vulnerabilities

If you identify a security vulnerability in one of our products or services, please report it via email to:

security@troester.de

Please include the following information in your report:

- **Reporter name:** (If you prefer to remain anonymous, we will respect your decision.)
  - Otherwise: email address and telephone number where we can reach you
  - Affiliation: your organization (if applicable)

- **Type of vulnerability:** How would you describe the vulnerability (e.g., XSS, buffer overflow, hard-coded credentials)?

- **Brief description:** A short explanation of the vulnerability (without technical details) and how you discovered it.

- **Affected components:** In which products, solutions, or services did you find the vulnerability? Include all available information such as product family and group, firmware or software version. For services, specify the relevant location (e.g., URL).

- **Triggering the vulnerability:** Can you provide code demonstrating the vulnerability (Proof of Concept, PoC)? Alternatively, you may submit network traces (e.g., pcaps) or a description of how to reproduce the vulnerability.

- **Impact:** Have you observed any effects caused by the vulnerability?

- **Confidentiality:** Has the vulnerability already been disclosed, or do you have concrete plans for disclosure?

Any design or implementation issue may be reported if it is reproducible and affects information, product, or IT security.

Please note that the following vulnerabilities are not covered by this policy:

- Attacks that require physical access to a user's device or network
- Reports from automated tools or scans without explanatory documentation
- The operator's failure to implement best practices

3. TROESTER Commitment

- We will acknowledge receipt of your report within 3 business days (based on Germany, Hanover).
  We will also keep you informed on an ongoing basis about the relevant steps taken as part of the processing.

- We will analyze and assess reported vulnerabilities, develop appropriate measures to address them, and communicate these in a coordinated manner.

- We will treat your report confidentially and will not disclose your personal data to third parties without your consent.