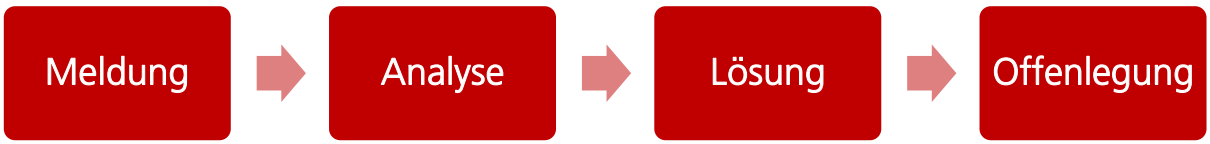
Leitfaden zum Umgang mit Sicherheitslücken

Vulnerability Handling Guideline

Verantwortlich für die Annahme, Bewertung und Bearbeitung sicherheitsrelevanter Meldungen, die Produkte und Dienstleistungen von TR Electronic betreffen, ist das Product Security Incident Response Team (PSIRT). Ziel ist es, potenzielle Schwachstellen schnell, transparent und verantwortungsvoll zu behandeln, um die Sicherheit unserer Kunden und Produkte jederzeit zu gewährleisten. Dieses Dokument beschreibt den standardisierten Prozess, nach dem unser PSIRT bei eingehenden Meldungen vorgeht.



1. Meldung

Potenzielle Schwachstellen können dem TR Electronic PSIRT unter psirt@tr-electronic.de gemeldet werden. Details zur Kontaktaufnahme sowie dem Inhalt einer Meldung sind unter https://www.tr-electronic.de/psirt aufgeführt. Nach Eingang bestätigt das PSIRT den Erhalt der Meldung und eröffnet einen internen Vorgang zur weiteren Bearbeitung.

2. Analyse

Das PSIRT führt eine technische Bewertung der gemeldeten Schwachstelle durch. Dies beinhaltet:

- Reproduzierbarkeit der Schwachstelle
- Bewertung des Schweregrads der Schwachstelle
- Identifikation betroffener Komponenten oder Produktversionen
- Einschätzung möglicher Risiken für Kunden und Systeme

Das PSIRT informiert den Berichterstatter über das Ergebnis der Analyse und vereinbart gegebenenfalls eine gemeinsame Vorgehensweise.

TR Electronic GmbH
Eglishalde 6
D-78647 Trossingen
Ust-ID-Nr. DE 142 929 277
Steuernummer / Fax number: 21060/51415

Telefon / Phone: +49 7425 228-0
Telefax / Fax: +49 7425 228-33
info@tr-electronic.de
www.tr-electronic.de

Amtsgericht
Stuttgart HRB 460 344
Geschäftsführer / Managing director:
Klaus Tessari
Andreas Thanassakis

Kreissparkasse Tuttlingen BIC SOLA DE S1 TUT
IBAN DE61 6435 0070 0000 0144 50
Deutsche Bank VS Schwenningen BIC DEUTDE6F694
IBAN DE58 6947 0039 0068 5222 00
Postbank Stuttgart BIC PBNKDEFF
IBAN DE73 6001 0070 0007 8887 07

3. Lösung

Nach Abschluss der Analyse entwickelt das verantwortliche Produktteam geeignete Maßnahmen zur Behebung der Schwachstelle. Dies kann umfassen:

- Software-Updates oder Patches
- Konfigurationsanpassungen
- Ergänzende Sicherheitsmechanismen
- Dokumentations- oder Prozessverbesserungen

Das PSIRT koordiniert und Unterstützt die Umsetzung. Kunden werden über verfügbare Security-Updates und empfohlene Maßnahmen informiert.

4. Offenlegung

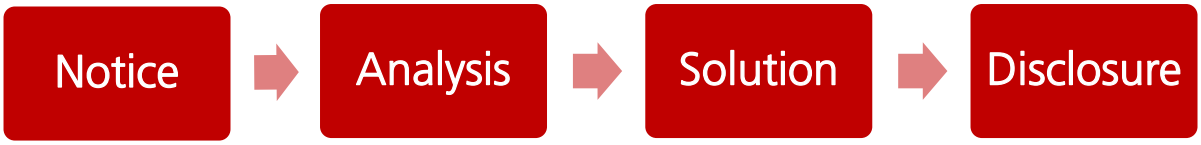
Sind die Arbeiten an einer Schwachstelle beendet, so wird diese veröffentlicht, je nach Schwere entweder per Release Note oder per Sicherheits-Advisory unter https://www.tr-electronic.de/psirt. Eine Ofenlegung umfasst typischerweise:

- Beschreibung der Schwachstelle
- Betroffene Produkte und Versionen
- Schweregradbewertung
- Verfügbare Updates oder empfohlene Maßnahmen

Die Offenlegung erfolgt in Abstimmung mit allen beteiligten Parteien, um sicherzustellen, dass Kunden ausreichend Zeit und Informationen erhalten, um ihre Systeme zu schützen.

Vulnerability Handling Guideline

The Product Security Incident Response Team (PSIRT) is responsible for receiving, assessing and handling security-related reports concerning TR Electronic's products and services. The aim is to address potential vulnerabilities quickly, transparently and responsibly in order to ensure the security of our customers and products at all times. This document describes the standardized process followed by our PSIRT when handling incoming reports.



1. Notice

Potential vulnerabilities can be reported to the TR Electronic PSIRT at psirt@tr-electronic.de. Details on how to contact us and what to include in a report can be found at https://www.tr-electronic.de/psirt. Upon receipt, the PSIRT will confirm receipt of the report and open an internal case for further processing

2. Analysis

The PSIRT carries out a technical assessment of the reported vulnerability. This includes:

- Verifying whether the vulnerability can be reproduced
- Assessing the severity of the vulnerability
- Identifying affected components or product versions
- Evaluating potential risks to customers and systems

The PSIRT informs the reporter of the outcome of the analysis and, where appropriate, agrees on a joint course of action.

3. Solution

Once the analysis is complete, the relevant product team develops appropriate measures to address the vulnerability. These may include:

- Software updates or patches
- Configuration changes
- Additional security mechanisms
- Improvements to Documentation or Processes

The PSIRT coordinates and supports the implementation. Customers are informed about available security updates and recommended measures.

4. Disclosure

Once work on a vulnerability has been completed, it is published, either as a release note or a security advisory, depending on its severity, at https://www.tr-electronic.de/psirt. A disclosure typically includes:

- Description of the vulnerability
- Affected products and versions
- Severity rating
- Available updates or recommended actions
-

The disclosure is made in consultation with all parties involved to ensure that customers are given sufficient time and information to protect their systems.