Murrelektronik Vulnerability Handling Process

Table of Contents

Scope and purpose of this document

This document describes the vulnerability handling process at Murrelektronik. It is intended to give all users of our products and solutions all the information they need to be prepared to deal with any cybersecurity issues or vulnerabilities that are discovered in our products.

Overview of the vulnerability handling process

Normative underpinning:

Murrelektronik is committed to implementing all necessary processes according to industry standards and applicable laws. This vulnerability handling process fulfills the requirements of IEC/ISO 62443 and ISO/IEC 29147:2014. It also fulfills the obligations under the EU CRA (Cyber Resilience Act).

Description of the process

The process is started when a vulnerability is reported, either from an external source or through the continuous internal monitoring performed by internal stakeholders (R&D, test, etc) or by external testing service providers acting on behalf of Murrelektronik.

The report is acknowledged, and an initial assessment takes place. PSIRT is the coordinator of this process externally and internally and it maintains communication with all stakeholders.

When the vulnerability is verified and analyzed, PSIRT coordinates with all stakeholders to develop remediation. This is followed by publishing a security advisory using the various channels defined in section “Disclosure” below.

A graphical presentation of this process can be found in fig. 1 below. The following sections present the details of the different phases of the process and give further information.

Fig. 1 Vulnerability handling process at Murrelektronik

Vulnerability Awareness

Internal monitoring and internal reporting

Murrelektronik has internal processes in place to continuously monitor, verify and validate our products for vulnerability. Eventual vulnerabilities that get discovered internally are handled in the same way that externally reported vulnerabilities are handled. This includes vulnerabilities discovered through testing commissioned by Murrelektronik but performed at external laboratories.

Contact

The preferred method of contact to report vulnerabilities is using encrypted E-Mail communication. PSIRT E-Mail address is: psirt@murrelektronik.de. Our current PGP key and key fingerprint can be found on the PSIRT web page under murrelektronik.com

Information to be included when reporting a vulnerability

To help us process vulnerability reports efficiently we would appreciate the inclusion of the following information:

- Affected product (including hardware and firmware or software version
- class or type of vulnerability, optionally using a taxonomy like CWE
- possible root cause
- Description of the vulnerability including a description how it can be reproduced. Inclusion of exploit code and/or network traces would be highly appreciated
- If the vulnerability is based on disclosed vulnerabilities in third party software component, please provide a link to the original disclosure.
- Information about active exploitation of the vulnerability, if applicable
- impact and severity estimate
- scope assessment, other products, components, services, or vendors thought to be affected
- disclosure plans, specifically embargo and publication timelines.
- Consent to include you in the acknowledgement section when publishing a security supervisory

Verification and analysis

When a vulnerability report is received and acknowledged, PSIRT starts the internal processes already established in the Murrelektronik to handle cybersecurity vulnerabilities. This includes an extensive list of tests and checks designed to understand the extent of the vulnerability and the risks associated with it. PSIRT coordinates with internal and external stakeholders and allocates the resources necessary for the effective and timely handling of the vulnerability.

Remediation

As soon as the vulnerability is verified the internal processes in the Murrelektronik kick in to handle the issue in a timely manner. PSIRT coordinates this effort with internal and external stakeholders. Normally one or more of the following types of remedies are developed:

- **Workaround**: Steps that the customer or user can take to prevent or reduce the possibility of the exploitation of the vulnerability.
- **Hotfix**: A Software patch that provides a quick fix to the vulnerability or makes exploiting it harder or impossible.
- **Updated software version**: A new software version is developed, that provides a comprehensive solution to the security issue following the company's established change management processes.
- **Updated user documentation**: If the issue cannot be solved by modifying the product's hardware or software then the documentation is updated to include the new information and possible steps that users can take to eliminate the risks.

Disclosure

Murrelektronik is committed to working on our customers, supplier and other stakeholders to find timely solutions to any security issues our products and solutions may have. We are also committed to fulfilling all the requirements of applicable laws and industry standards, especially when it comes to the deadlines defined for the disclosure of vulnerabilities. We are also committed to working closely with the reporter of the vulnerability to guarantee a safe and responsible disclosure of vulnerabilities in order to enable the users to remediate the issues before they get exploited, whenever possible.

Contents of ME security advisory

The goal of our security advisories is to provide our customers with timely information on vulnerabilities, so they can quickly establish if they are affected by them and how best to react. They contain information that address the needs of technical and non-technical readers alike. Our advisories are provided in English.

The advisories we publish normally contain most or all of the following elements:

1. **Advisory ID**
2. **Date and time** of initial publication, and a revision history if updates to the advisory are made.
3. **Title:** including enough information (for example about the affected product) to enable the reader to quickly decide if the advisory is relevant.
4. **Overview**: a short general description of the vulnerability.
5. **Affected products**: including product name(s), affected hardware and firmware version(s) and if applicable a safe way to test for the presence of the vulnerability.

6. **Description**: containing just enough details to enable the users to assess their risks without making exploitation easier or more likely. The class and CVSS score may be included in the description.
7. **Impact**: To include the potential consequences if the discovered vulnerability is exploited and the attack scenarios it enables.
8. **Severity**: A classification of the vulnerability according to the Common Vulnerability Scoring System (CVSS).
9. **Remediation**: The steps users can take to reduce or prevent the exploitation of the vulnerability (workarounds) and the steps required to remove the vulnerability (e.g. by installing software patches or updates).
10. **References** to related information, like related advisories or CVE (Common Vulnerabilities and Exposures.
11. Acknowledgement of the reporters of the vulnerability, if applicable.
12. **Contact information** of Murrelektronik PSIRT
13. **Terms of use**: Terms for copywrite and redistribution.

Publishing:

The security advisories published by Murrelektronik can be accessed using several channels:

Website: Our PSIRT web page has a list the most recent and active advisories. It also contains a link to the archive of all published advisories

CERT@VDE: We post our advisories to the CERT@VDE database.

Newsletter: You can subscribe to our newsletter and receive timely information and updates not only about recently published advisories, but also about all the activities related to cybersecurity at Murrelektronik.