SICK AG Vulnerability Handling Guideline

SICK PSIRT welcomes reports of vulnerabilities from anyone, regardless of their customer status, and investigates them diligently. Among others, reporters include safety researchers, universities, CERTs, business partners, authorities, industry associations and suppliers. Uncovering vulnerabilities is understood as a common goal of different parties with the aim of offering our customers a consistently high level of security. This is particularly important because SICK AG products fulfill important protective functions and are used in critical infrastructures. This document describes the process transparently to encourage all parties to make coordinated reports on vulnerabilities.

During the entire process, SICK PSIRT aims to work together with all affected parties both professionally and with trust. If you have questions about this document, SICK PSIRT can provide information at psirt@sick.de. You can contact us in German or English.

The steps of the process are:

Report

SICK PSIRT receives a vulnerability report. Information on contacting us and the contents of a report can be found at https://www.sick.com/psirt. Neither a non-disclosure agreement (NDA) nor another type of contract is necessary or a requirement for collaboration.

Analysis

SICK PSIRT formally examines all incoming reports for relevance and completeness. These are then forwarded to the respective development areas and examined. If necessary, partners or other CERTs are informed and involved in the process. Regular communication with the reporter takes place.

Solution

The areas responsible for the product develop a solution to appropriately handle the risk of the vulnerability. SICK PSIRT coordinates and supports all activities. If appropriate, a solution can be provided to the reporter in advance for examination.

Disclosure

SICK PSIRT discloses the vulnerability in a coordinated event in the final step. The security advisory provides a description of the vulnerability along with recommendations to mitigate the resulting risk. The reporter can be acknowledged publicly if the process of a coordinated vulnerability disclosure was followed.