of offering our customers a consistently high level of security.

The SICK Product Security Incident Response Team (SICK PSIRT)

The SICK PSIRT is the central team of SICK AG which is authorized to answer reports regarding the cyber security of products, solutions and services as well as provide information. All reports concerning potential vulnerabilities or other security incidents connected to SICK AG products can be passed on to the SICK PSIRT.

The SICK PSIRT manages the inspection, internal coordination and disclosure of security vulnerabilities. A security advisory is issued for confirmed vulnerabilities as soon as a solution is available. If the situation requires, a security advisory with the measures to be taken is sent out before an update is available.

Reports on potential vulnerabilities or other incidents are more than welcome from anyone, regardless of their customer status. SICK AG respects and takes into account the different interests of reporters and encourages the reporting of information to the SICK PSIRT. The aim is to follow a process of coordinated disclosure of vulnerabilities (coordinated vulnerability disclosure).

Handling vulnerabilities is described in document “Vulnerability Handling Guideline”.

Reporting a vulnerability

The SICK PSIRT aims to process every vulnerability with confidentiality and professionalism together with the respective reporters. Neither a non-disclosure agreement (NDA) nor another type of contract is necessary or a requirement for collaboration.

Coordinated vulnerability reports from all members of the security community are greatly appreciated. These include security researchers, universities, CERTs, business partners, authorities, industry associations and suppliers.

Many SICK AG products fulfill important protective functions and are used in critical infrastructures. SICK AG therefore asks for cooperation when dealing with the coordinated disclosure of vulnerabilities and also requests that vulnerability information not be disclosed prematurely.

SICK AG requests that as much information as possible is provided in a report in order to speed up processing. This information should contain the following:

- **Contact information and availability**
- **Affected product including model and version number**
- **Classification of the vulnerability** (buffer overflow, XSS, ...)
- **Detailed description of the vulnerability** (with verification if possible)
- **Effect of the vulnerability** (if know)
- **Current level of awareness of the vulnerability** (are there plans to disclose it?)
- **(Company) affiliation of the reporter** (if reporter is prepared to provide such information)
- **CVSS score** (if known)

If more information is necessary for the inspection of a vulnerability, the SICK PSIRT will contact the reporter.

If the reporter would like, he/she will be publicly acknowledged after disclosing a new vulnerability.

Contact information

Reports for the SICK PSIRT are to be sent to this address:

- psirt@sick.de
  (PGP Public Key with fingerprint: E509 7FC0 4047 3BB3 0F3E A7E0 D586 2240 0E6D 0E90)
- Accepted languages: German and English
- Transmission: Encryption preferred

Encrypted reports are preferred to protect sensitive information and data. German and English are accepted.

The SICK PSIRT is happy to provide additional information about its operating principle or answer general questions about reports of vulnerabilities. If you have any other questions or concerns not related to security, we ask that you contact SICK AG customer service. The SICK PSIRT cannot provide in

Security Advisories

2026

ID	Title	CVSS Score	Products	Date	Download	Signature
SCA-2026-0001	Vulnerabilities affecting SICK TDC-X401GL	9.9	SICK TDC-X401GL	15.01.2026	Download PDF Download JSON	Download
SCA-2026-0002	Vulnerabilities affecting SICK Incoming Goods Suite	8.3	SICK Incoming Goods Suite	15.01.2026	Download PDF Download JSON	Download
SCA-2026-0003	Vulnerability affecting SICK nanoScan3 and microScan3	5.3	SICK microScan3 Pro I/O, SICK microScan3 EtherCAT, SICK nanoScan3 Core I/O, SICK nanoScan3 Pro I/O	26.01.2026	Download PDF Download JSON	Download
SCA-2026-0004	Eclipse Cyclone DDS Vulnerabilities have no impact on SICK picoScan150 & SICK picoScan120 products	10	SICK picoScan150, SICK picoScan120	13.02.2026	Download PDF Download JSON	Download
SCA-2026-0005	Vulnerabilities affecting SICK LMS1000 and SICK MRS1000	6.5	SICK LMS1000, SICK MRS1000	27.02.2026	Download PDF Download JSON	Download

SCA-2026-0006	Vulnerabilities affecting SICK Lector85x and SICK Lector83x	9.8	SICK Lector85x, SICK Lector83x	06.03.2026	Download PDF Download JSON	Download
SCA-2026-0007	Sudo vulnerability affects Endress+Hauser MCS200HW	9.8	Endress+Hauser MCS200HW	21.04.2026	Download PDF Download JSON	Download

2025 +

2024 +

2023 +

2022 +

2021 +

2020 +

2019 +

History

08/19/2024 - Update of the PGP Public Key. The previous key can be downloaded here.

09/18/2024 - Update of the PGP Public Key. The previous key can be downloaded here.

09/22/2023 - Update of the PGP Public Key. The previous key can be downloaded here.

08/09/2022 - Update of the PGP Public Key. The previous key can be downloaded here.

09/21/2021 - Update of the PGP Public Key. The previous key can be downloaded here.

09/24/2020 - Update of the PGP Public Key. The previous key can be downloaded here.

18/10/2019 - Update of the PGP Public Key. The previous key can be downloaded here.

12/10/2018 - Introduction of the SICK PSIRT

Contact

SICK PSIRT – cyber security contact for SICK products

psirt@sick.de

Reports can be sent in German or English.

Security Advisories

› SICK Security Advisories

If you prefer RSS to stay up-to-date, subscribe to our feed:

All SICK Security Advisories

Documents

› PGP Public Key with fingerprint: E509 7FC0 4047 3BB3 0F3E A7E0 D586 2240 0E6D 0E90

Vulnerability Handling Guideline

Acknowledgments

› Acknowledgments

Type: Flyer

Part number: -

Title: COMPLETELY SECURED Industrial Information Security

Release date: Jul 29, 2019

Size: 2.68 MB

English

Add to wish list

Download

Type: Special information

Part number: -

Title: SICK OPERATING GUIDELINES - CYBERSECURITY BY SICK

Release date: Jul 29, 2019

Size: 1.00 MB

English

Add to wish list

Download

Further information

- BSI

- ICS-Cert
- ISA
- IEC