TLP:WHITE

SICK PSIRT
Security Advisory

Critical vulnerabilities in SICK InspectorP61x, InspectorP62x and TiM3xx

Document ID:	SCA-2024-0006
Publication Date:	2024-12-06
CVE Identifiers:	CVE-2024-10771, CVE-2024-10772, CVE-2024-10773, CVE-2024-10774, CVE-2024-10776, CVE-2024-11022
Version:	1

Summary

Multiple critical vulnerabilities were found in the SICK products InspectorP61x, InspectorP62x and TiM3xx. If exploited, this potentially allows an attacker to impact availabiltiy, integrity and confidentaility of the products. It is strongly recommended to upgrade the InspectorP61x, InspectorP62x and TiM3xx to the latest release.

List of Products

Product	Affected by
SICK InspectorP61x all firmware versions	CVE-2024-11022 Status: Known Affected Remediation: Workaround
SICK InspectorP61x with Firmware <5.0.0	CVE-2024-10771 Status: Known Affected Remediation: Vendor fix
	CVE-2024-10772 Status: Known Affected Remediation: Vendor fix
	CVE-2024-10773 Status: Known Affected Remediation: Vendor fix

	CVE-2024-10774 Status: Known Affected Remediation: Mitigation
	CVE-2024-10776 Status: Known Affected Remediation: Mitigation
SICK InspectorP62x all firmware versions	CVE-2024-11022 Status: Known Affected Remediation: Workaround
SICK InspectorP62x with Firmware <5.0.0	CVE-2024-10771 Status: Known Affected Remediation: Vendor fix
	CVE-2024-10772 Status: Known Affected Remediation: Vendor fix
	CVE-2024-10773 Status: Known Affected Remediation: Vendor fix
	CVE-2024-10774 Status: Known Affected Remediation: Mitigation
	CVE-2024-10776 Status: Known Affected Remediation: Mitigation
SICK TiM3xx with Firmware <5.10.0	CVE-2024-10771 Status: Known Affected Remediation: Workaround
	CVE-2024-10773 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2024-10771 Improper Control of Generation of Code (’Code Injection’)

Summary: Due to missing input validation during one step of the firmware update process, the product is vulnerable to remote code execution. With network access and the user level ”Service”, an attacker can execute arbitrary system commands in the root user’s contexts.

CVE-2024-10771 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-94 (Improper Control of Generation of Code (’Code Injection’))

CVE-2024-10772 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking

Summary: Since the firmware update is not validated, an attacker can install modified firmware on the device. This has a high impact on the availabilty, integrity and confidentiality up to the complete compromise of the device.

CVE-2024-10772 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-649 (Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking)

CVE-2024-10773 Hidden Functionality

Summary: The product is vulnerable to pass-the-hash attacks in combination with hardcoded credentials of hidden user levels. This means that an attacker can log in with the hidden user levels and gain full access to the device.

CVE-2024-10773 has been assigned to this vulnerability.
CVSSv3.1 base score: 9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-912 (Hidden Functionality)

CVE-2024-10774 Missing Authentication for Critical Function

Summary: Unauthenticated CROWN APIs allow access to critical functions. This leads to the accessibility of large parts of the web application without authentication.

CVE-2024-10774 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

CVE-2024-10776 Missing Authentication for Critical Function

Summary: Lua apps can be deployed, removed, started, reloaded or stopped without authorization via AppManager. This allows an attacker to remove legitimate apps creating a DoS attack, read and write files or load apps that use all features of the product available to a customer.

CVE-2024-10776 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

CVE-2024-11022 Reusing a Nonce, Key Pair in Encryption

Summary: The authentication process to the web server uses a challenge response procedure which inludes the nonce and additional information. This challenge can be used several times for login and is therefore vulnerable for a replay attack.

CVE-2024-11022 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
CWE identifier: CWE-323 (Reusing a Nonce, Key Pair in Encryption)

Remediations

Vendor Fix for CVE-2024-10771

Details: Customers are strongly recommended to upgrade to the latest release.

Valid for:

- SICK InspectorP61x with Firmware <5.0.0
- SICK InspectorP62x with Firmware <5.0.0

Workaround for CVE-2024-10771

Details: We recommend updating the firmware only in a trusted environment.

Valid for:

- SICK TiM3xx with Firmware <5.10.0

Vendor Fix for CVE-2024-10772

Details: Customers are strongly recommended to upgrade to the latest release.

Valid for:

- SICK InspectorP61x with Firmware <5.0.0
- SICK InspectorP62x with Firmware <5.0.0

Vendor Fix for CVE-2024-10773

Details: Customers are strongly recommended to upgrade to the latest release.

Valid for:

- SICK InspectorP61x with Firmware <5.0.0
- SICK InspectorP62x with Firmware <5.0.0
- SICK TiM3xx with Firmware <5.10.0

Mitigation for CVE-2024-10774

Details: Customers are strongly recommended to upgrade to the latest release. Furthermore, the app development for which the CROWN API is required should be done in a trusted environment. As soon as the device is used productively with the custom-developed apps, the CROWN API should be deactivated.

Valid for:

- SICK InspectorP61x with Firmware <5.0.0
- SICK InspectorP62x with Firmware <5.0.0

Mitigation for CVE-2024-10776

Details: Customers are strongly recommended to upgrade to the latest release. Furthermore, the app development should be done in a trusted environment. After the development, app management should be disabled.

Valid for:

- SICK InspectorP61x with Firmware <5.0.0
- SICK InspectorP62x with Firmware <5.0.0

Workaround for CVE-2024-11022

Details: As the communication is not encrypted, the device should only be used in a trusted environment.

Valid for:

- SICK InspectorP61x all firmware versions
- SICK InspectorP62x all firmware versions

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Acknowledgments

Thanks to Manuel Stotz and Tobias Jäger from SySS GmbH for pentesting the products and reporting the vulnerabilities (URL: https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2024-053.txt, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2024-054.txt, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2024-055.txt, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2024-056.txt).

History

Version	Release Date	Comment
1	2024-12-06	Initial version