Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Security Information Regarding ”Profile Programming”

Document ID:	SCA-2020-0001
Publication Date:	2020-05-31
CVE Identifier:	N/A (CWE-15)
Version:	2

Summary

The customer IOActive provided a Security Advisory report to SICK AG referring to the feature profile programming with regards to the listed affected products. Certain SICK products support profile programming with bar codes, generated and printed via SOPAS ET.

List of Products

Product	Affected by
SICK CLV62x with Firmware <=6.10	External Control of System or Configuration Setting Status: Known Affected Remediation: Mitigation
SICK CLV63x with Firmware <=6.10	External Control of System or Configuration Setting Status: Known Affected Remediation: Mitigation
SICK CLV64x with Firmware <=6.10	External Control of System or Configuration Setting Status: Known Affected Remediation: Mitigation
SICK CLV65x with Firmware <=6.10	External Control of System or Configuration Setting Status: Known Affected Remediation: Mitigation

Vulnerability Overview

External Control of System or Configuration Setting

Summary: The functionality profile programming relies in custom CODE128 bar codes that once scanned will trigger certain actions in the device, which can be leveraged to change configuration settings. These custom barcodes do not implement any kind of authentication, so once bar codes are generated, they will work on any SICK device that support them.
As a result, an attacker that is able to physically present a malicious ”profile programming” bar code to the affected device can either render it inoperable or change settings to facilitate further attacks.

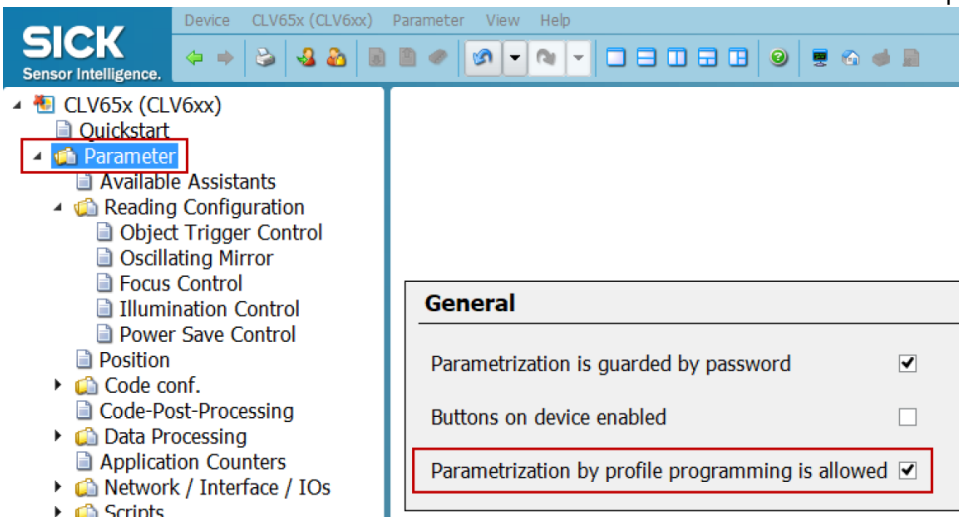
No CVE has been assigned to this vulnerability.
CWE identifier: CWE-15 (External Control of System or Configuration Setting)

Impact: An attacker with the ability to present special barcodes under his control to the affected devices, with enabled ”profile programming”, is able to change the configuration without any authentication required. This could lead to an impact on availability, integrity and confidentiality. The configuration is not possible if ”Parametrization by profile programming is allowed” is disabled.

Remediations

Mitigation for External Control of System or Configuration Setting

Details: Deactivation of profile programming Profile programming is active by factory default. To deactivate the feature a login via user level ”service” is required. In parameter tree section, ”Parameter” under the area ”General” the user is able to select enable or disable the feature ”profile programming”.



Valid for:

- SICK CLV62x with Firmware <=6.10
- SICK CLV63x with Firmware <=6.10
- SICK CLV64x with Firmware <=6.10
- SICK CLV65x with Firmware <=6.10

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:
http://ics-cert.us-cert.gov/content/recommended-practices

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

Acknowledgments

Thanks to Ruben Santamarta, Principal Security Consultant from IOActive for his research and the report.

Additional Product Information

SICK CLV62x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv62x/c/g79824
SICK CLV63x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv63x/c/g79846
SICK CLV64x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv64x/c/g79874
SICK CLV65x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv65x/c/g79879

History

Version	Release Date	Comment
1	2020-05-31	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)