

SICK PSIRT

Security Advisory

SECURITY INFORMATION REGARDING „Profile Programming“

Document ID: SCA-2020-0001
Publication Date: 2020-05-31

SUMMARY

The customer IOActive provided a Security Advisory report to SICK AG referring to the feature profile programming with regards to the listed products in section PRODUCTS USING “Profile Programming”. Certain SICK products support profile programming with bar codes, generated and printed via SOPAS ET.

This functionality relies in custom CODE 128 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.

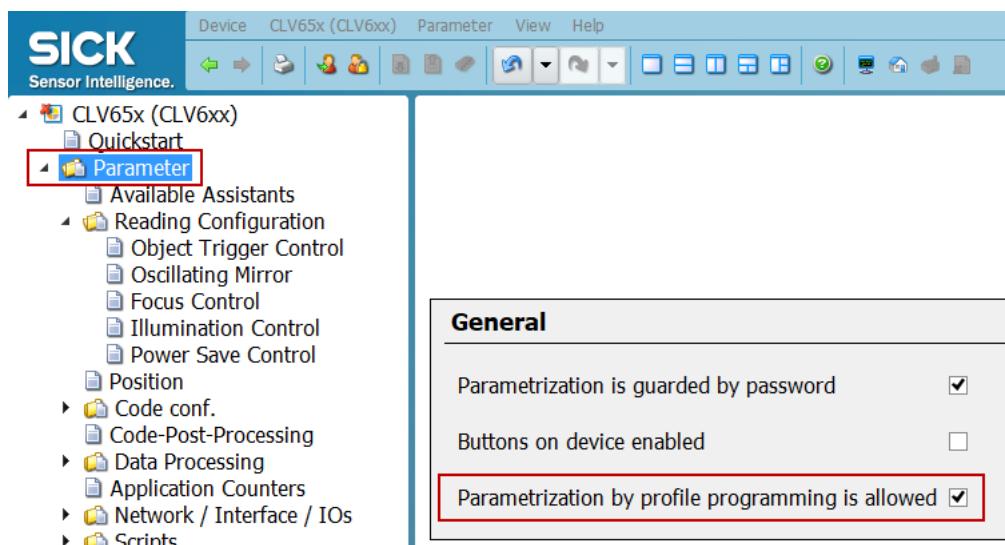
PRODUCTS USING “Profile Programming”

Product	Version	Remediation available
CLV62x ... CLV65x	All versions – current release V6.10	Yes – Deactivation of profile programming

SOLUTION

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”



POTENTIAL RISK

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.

ACKNOWLEDGMENTS

We want to thank Ruben Santamarta, Principal Security Consultant at IOActive for his research and the report.

RESOURCES

SICKSupportPortal: <https://supportportal.sick.com/tutorial/profile-programming-clv/>

HISTORY

Version	Release Date	Comment
V1	2020-05-31	Initial Release