

SICK PSIRT Security Advisory

Vulnerability in FX0-GENT00000 and FX0-GPNT00000

Document ID: SCA-2019-0002
Publication Date: 2019-09-20
CVSSv3 Base Score: 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:U/RC:C/CR:H)
CVE Identifier: CVE-2019-14753
Version: V1.0

SUMMARY

The security-testlab team of Fraunhofer IOSB in Karlsruhe reported a security vulnerability that affects FX0-GPNT00000 and FX0-GENT00000 in the version V3.04.0. The FX0-GPNT00000 and FX0-GENT00000 are vulnerable to a buffer overflow by exploiting the available resources with UDP packets, causing the Flexi Soft System to switch to safety state.

Currently SICK is not aware of any public exploits specifically targeting this vulnerability.

SICK has released a new firmware version for the FX0-GPNT00000 and FX0-GENT00000 and recommends using the new version.

AFFECTED PRODUCTS

Product	Version	Remediation available
FX0-GPNT00000 (1044074)	V3.04.0	New version V3.05.0
FX0-GENT00000 (1044072)	V3.04.0	New version V3.05.0

SOLUTION

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.

Additional information on Industrial Security can be found at:

<https://sick.com/psirt>

Please contact your local SICK Sales and Service for further steps.

VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.0). 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.

ACKNOWLEDGMENTS

The security-testlab team of Fraunhofer IOSB in Karlsruhe reported this vulnerability to SICK.

RESOURCES

CVSS Calculator

<https://www.first.org/cvss/calculator/3.0#>

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

HISTORY

Version	Release Date	Comment
V1.0	2019-09-20	Initial Release