SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK FX0-GENT00000 and SICK FX0-GPNT00000

Document ID:	SCA-2019-0002
Publication Date:	2019-09-20
CVE Identifier:	CVE-2019-14753
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:U/RC:C/CR:H
Version:	2

Summary

The security-testlab team of Fraunhofer IOSB in Karlsruhe reported a security vulnerability that affects SICK FX0-GPNT00000 and SICK FX0-GENT00000 in the version V3.04.0. The SICK FX0-GPNT00000 and SICK 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 SICK FX0-GPNT00000 and SICK FX0-GENT00000 and recommends using the new version.

List of Products

Product	Part Number	Affected by
SICK FX0-GENT00000 with Firmware 3.04.0	1044072	CVE-2019-14753 Status: Known Affected Remediation: Vendor fix
SICK FX0-GPNT00000 with Firmware 3.04.0	1044074	CVE-2019-14753 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2019-14753 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability summary: The SICK FX0-GPNT00000 and SICK 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.

CVE-2019-14753 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:U/RC:C/CR:H
CWE identifier: CWE-120 (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))

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

Valid for:

- SICK FX0-GENT00000 with Firmware 3.04.0
- SICK FX0-GPNT00000 with Firmware 3.04.0

Remediations

Vendor Fix for CVE-2019-14753

Details: SICK has released a new firmware version for the FX0 GPNT00000 and SICK FX0-GENT00000 and recommends using the new version V3.05.0.

Valid for:

- SICK FX0-GENT00000 with Firmware 3.04.0
- SICK FX0-GPNT00000 with Firmware 3.04.0

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

Additional Product Information

SICK FX0-GENT00000 with Firmware 3.04.0	Product on sick.com: https://www.sick.com/de/de/p/p80485
SICK FX0-GPNT00000 with Firmware 3.04.0	Product on sick.com: https://www.sick.com/de/de/p/p80487

History

Version	Release Date	Comment
1	2019-09-20	Initial Release
2	2023-02-09	Updated Advisory (only visual changes)