SICK PSIRT
Security Advisory

Vulnerabilities in SICK MARSIC300

Document ID:	SCA-2022-0007
Publication Date:	2022-04-21
CVE Identifiers:	CVE-2016-7406, CVE-2016-7407
Version:	V2.0

SUMMARY

SICK received a report about multiple security vulnerabilities in the SICK MARSIC 300 device. The security vulnerabilities are caused by the third-party library Dropbear, which is used by the SICK MARSIC 300 to provide SSH communication. A successful exploitation of these vulnerabilities could lead to a remote code execution.
SICK has released a new version of the SICK MARSIC 300 firmware and recommends updating to the newest version.

AFFECTED PRODUCTS

Product	Version	Remediation available
SICK MARSIC 300	Prior to version **1EU4_220310**	Yes

VULNERABILITY OVERVIEW

CVE-2016-7406 Improper Input Validation
Format string vulnerability in Dropbear SSH before 2016.74 allows remote attackers to execute arbitrary code via format string specifiers in the (1) username or (2) host argument.

CVE-2016-7406 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2016-7407 Improper Input Validation
The dropbearconvert command in Dropbear SSH before 2016.74 allows attackers to execute arbitrary code via a crafted OpenSSH key file.

CVE-2016-7407 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

GENERAL SECURITY PRACTICES

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

VULNERABILITY CLASSIFICATION

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

HISTORY

Version	Release Date	Comment
V1	2022-04-21	Initial Version
V2	2022-04-22	Fixed TLP classification