

# 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: 4

### Summary

---

SICK received a report about multiple security vulnerabilities in the SICK MARSIC300 device. The security vulnerabilities are caused by the third-party library Dropbear, which is used by the SICK MARSIC300 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 MARSIC300 firmware and recommends updating to the newest version.

### List of Products

---

| Product   | Affected by  |
|---|--|
| <b>SICK MARSIC300 with Firmware &lt;1EU4.220310</b> | <a href="#">CVE-2016-7406</a><br>Status: Known Affected<br>Remediation: Vendor fix |
|   | <a href="#">CVE-2016-7407</a><br>Status: Known Affected<br>Remediation: -          |

## Vulnerability Overview

---

### CVE-2016-7406 Improper Input Validation

**CVE Description:** 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

CWE identifier: CWE-20 (Improper Input Validation)

**References:**

CVE Entry:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7406>

### CVE-2016-7407 Improper Input Validation

**CVE Description:** 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

CWE identifier: CWE-20 (Improper Input Validation)

**References:**

CVE Entry:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7407>

## Remediations

---

### Vendor Fix for CVE-2016-7406

Details: SICK has released a new version of the SICK MARSIC300 firmware and recommends updating to the newest version.

Valid for:

- SICK MARSIC300 with Firmware <1EU4\_220310

## 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://www.sick.com/media/docs/9/19/719/special\\_information\\_sick\\_operating\\_guidelines\\_cybersecurity\\_by\\_sick\\_en\\_im0106719.pdf](https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.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>

## Additional Product Information

---

**SICK MARSIC300 with Firmware <1EU4 220310** Product on sick.com: <https://www.sick.com/de/de/p/p475061>



Sensor Intelligence.

**TLP:WHITE**

## History

---

| Version | Release Date | Comment  |
|---------|--------------|--|
| 1       | 2022-04-21   | Initial Release  |
| 2       | 2022-04-22   | Fixed TLP classification   |
| 3       | 2023-02-10   | Updated Advisory (only visual changes)                               |
| 4       | 2025-07-30   | Updated Advisory: URL for SICK Operating Guidelines has been updated |

**TLP:WHITE**