SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

MSC800 affected by hard-coded credentials vulnerability

Document ID:	SCA-2019-0001
Publication Date:	2019-06-21
CVE Identifier:	CVE-2019-10979
CVSSv3 Base Score:	9.8
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Version:	2

Summary

The ICS-CERT reported a security vulnerability that affects MSC800 versions before 4.0. The MSC800 uses hard-coded credentials, which potentially allow low-skilled remote attackers to reconfigure settings and /or disrupt the functionality of the device.
Currently SICK is not aware of any public exploits specifically targeting this vulnerability.
SICK has released a firmware update for MSC800 and recommends updating to the new version.

List of Products

Product	Part Number	Affected by
SICK MSC800 with Firmware <4.0	1040571	CVE-2019-10979 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2019-10979 Use of Hard-coded Credentials

Vulnerability summary: The MSC800 uses hard-coded credentials, which potentially allow low-skilled unauthorized remote attackers to reconfigure settings and /or disrupt the functionality of the device.

CVE-2019-10979 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-798 (Use of Hard-coded Credentials)

Impact: An attacker gaining access to a privileged account could execute code, read sensitive data, change configurations or disrupt the functionality of the product.

Valid for:

- SICK MSC800 with Firmware <4.0

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

Valid for:

- SICK MSC800 with Firmware <4.0

Remediations

Vendor Fix for CVE-2019-10979

Details: SICK has released a firmware update for MSC800 and recommends updating to the new version V4.0.
The update allows customers to change the default customer passwords and to optionally disable device configuration over desired networks interfaces, especially in critical infrastructures. The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person. Until the firmware update is installed, general security practices should be utilized. In case the referenced patches cannot be applied, the following general security practices could mitigate the associated risk.

Valid for:

- SICK MSC800 with Firmware <4.0

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

Additional Product Information

SICK MSC800 with Firmware <4.0	Product on sick.com: https://www.sick.com/de/de/p/p354746

History

Version	Release Date	Comment
1	2019-06-21	Initial Release
2	2023-02-09	Updated Advisory (only visual changes)