TLP:WHITE

SICK PSIRT
Security Advisory

Inadequate SSH configuration in SICK Visionary-S CX

Document ID:	SCA-2021-0001
Publication Date:	2021-06-25
CVE Identifier:	CVE-2021-32496
CVSSv3 Base Score:	3.7
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Version:	3

Summary

SICK received a report that informed SICK about an Inadequate Encryption Strength vulnerability in the SICK product “SICK Visionary-S CX” concerning the internal SSH interface solely used by SICK for recovering returned devices.
Currently SICK is not aware of any public exploits specifically targeting this vulnerability.

The vulnerability is not visible in any supported customer functionality. Thus customers can only identify products by firmware version. Accessing the device via SSH now shows OpenSSH instead of dropbear.

List of Products

Product	Affected by
SICK Visionary-S CX with Firmware <5.21.2.29154R	CVE-2021-32496 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2021-32496 Inadequate Encryption Strength

Description: The use of weak algorithms makes it easier for an attacker to break the security that protects information transmitted from the client to the SSH server, assuming the attacker has access to the network on which the device is connected. This can increase the risk that encryption will be compromised, leading to the exposure of sensitive user information and man-in-the-middle attacks. SICK has developed a hotfix. In released firmware versions greater than 5.21.2.29154 the SSH server will no longer offer these weak ciphers.

CVE-2021-32496 has been assigned to this vulnerability.
CVSSv3.1 base score: 3.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
CWE identifier: CWE-326 (Inadequate Encryption Strength)

Remediations

Vendor Fix for CVE-2021-32496

Details: Update to version 5.21.2.29154R or higher

Valid for:

- SICK Visionary-S CX with Firmware <5.21.2.29154R

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

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

BSI Technical Guideline for the use of the cryptographic protocol Secure Shell (SSH):
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-4.pdf

History

Version	Release Date	Comment
1	2021-06-26	Initial Release
2	2023-02-09	Updated Advisory (only visual changes)
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated