Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Use of a Broken or Risky Cryptographic Algorithm in SICK RFU6xx RADIO FREQUEN. SENSOR

Document ID:	SCA-2022-0015
Publication Date:	2022-12-08
CVE Identifiers:	CVE-2022-27581, CVE-2022-46832, CVE-2022-46833, CVE-2022-46834
Version:	2

Summary

SICK received a report about a vulnerability in the SICK RFU6XX RADIO FREQUEN. SENSOR.
The used SSH service allowed for weak cipher suites to be used in traffic encryption. If weak cipher suites are used for traffic encryption, an attacker could potentially decrypt the traffic, which would affect the confidentiality of the transferred data.
For the vulnerability to be exploited, the victim must request weak cipher suites from the SSH service to encrypt the data.
SICK has released a new version of the SICK RFU6XX RADIO FREQUEN. SENSOR. and recommends updating to the newest version.

List of Products

Product	Part Number	Affected by
SICK RFU610-10600 with Firmware <2.25	1091102	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10601 with Firmware <2.25	1099890	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10603 with Firmware <2.25	1104443	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10604 with Firmware <2.25	1104444	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10605 with Firmware <2.25	1101394	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10607 with Firmware <2.25	1104447	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10609 with Firmware <2.25	1104449	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10610 with Firmware <2.25	1104446	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10613 with Firmware <2.25	1104445	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10614 with Firmware <2.25	1104441	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU610-10618 with Firmware <2.25	1104448	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix

SICK RFU610-10700 with Firmware <2.25	1115779	CVE-2022-27581 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10100 with Firmware <2.21	1062599	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10101 with Firmware <2.21	1062602	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10102 with Firmware <2.21	1101700	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10103 with Firmware <2.21	1091355	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10104 with Firmware <2.21	1069677	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10105 with Firmware <2.21	1068728	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10107 with Firmware <2.21	1068727	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10108 with Firmware <2.21	1094605	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10111 with Firmware <2.21	1084997	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10114 with Firmware <2.21	1096414	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10118 with Firmware <2.21	1101686	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix

SICK RFU620-10400 with Firmware <2.21	1062600	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10401 with Firmware <2.21	1062603	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10500 with Firmware <2.21	1062601	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10501 with Firmware <2.21	1062604	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10503 with Firmware <2.21	1069453	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10504 with Firmware <2.21	1070407	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10505 with Firmware <2.21	1077860	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10507 with Firmware <2.21	1083976	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10508 with Firmware <2.21	1088871	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10510 with Firmware <2.21	1083557	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU620-10514 with Firmware <2.21	1077863	CVE-2022-46832 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04100 with Firmware <2.21	1058117	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix

SICK RFU630-04100S01 with Firmware <2.21	1064280	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04101 with Firmware <2.21	1059999	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04102 with Firmware <2.21	1073376	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04103 with Firmware <2.21	1104670	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04104 with Firmware <2.21	1093152	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04105 with Firmware <2.21	1073196	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04106 with Firmware <2.21	1068569	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04108 with Firmware <2.21	1070904	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04109 with Firmware <2.21	1073377	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-04117 with Firmware <2.21	1087776	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13100 with Firmware <2.21	1054396	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13100S01 with Firmware <2.21	1064279	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix

SICK RFU630-13101 with Firmware <2.21	1054397	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13102 with Firmware <2.21	1058775	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13103 with Firmware <2.21	1067473	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13104 with Firmware <2.21	1068726	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13105 with Firmware <2.21	1057943	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13106 with Firmware <2.21	1067133	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13107 with Firmware <2.21	1061498	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13108 with Firmware <2.21	1070903	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13110 with Firmware <2.21	1073442	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13111 with Firmware <2.21	1077862	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13113 with Firmware <2.21	1077861	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU630-13114 with Firmware <2.21	1095224	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix

SICK RFU630-13115 with Firmware <2.21	1083558	CVE-2022-46833 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10100 with Firmware <2.21	1073556	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10101 with Firmware <2.21	1076522	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10102 with Firmware <2.21	1087587	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10103 with Firmware <2.21	1096413	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10104 with Firmware <2.21	1092036	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10105 with Firmware <2.21	1083559	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix
SICK RFU650-10106 with Firmware <2.21	1083560	CVE-2022-46834 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2022-27581 Use of a Broken or Risky Cryptographic Algorithm

CVE description: Use of a Broken or Risky Cryptographic Algorithm in SICK RFU61x firmware version < v2.25 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface.

CVE-2022-27581 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2022-46832 Use of a Broken or Risky Cryptographic Algorithm

CVE description: Use of a Broken or Risky Cryptographic Algorithm in SICK RFU62x firmware version $<$ 2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface.

CVE-2022-46832 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2022-46833 Use of a Broken or Risky Cryptographic Algorithm

CVE description: Use of a Broken or Risky Cryptographic Algorithm in SICK RFU63x firmware version $<$ v2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface.

CVE-2022-46833 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2022-46834 Use of a Broken or Risky Cryptographic Algorithm

CVE description: Use of a Broken or Risky Cryptographic Algorithm in SICK RFU65x firmware version $<$ v2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface.

CVE-2022-46834 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

Remediations

Vendor Fix for CVE-2022-27581

Details: The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.

Valid for:

- SICK RFU610-10600 with Firmware $<$2.25
- SICK RFU610-10601 with Firmware $<$2.25
- SICK RFU610-10603 with Firmware $<$2.25
- SICK RFU610-10604 with Firmware $<$2.25

- SICK RFU610-10605 with Firmware <2.25
- SICK RFU610-10607 with Firmware <2.25
- SICK RFU610-10609 with Firmware <2.25
- SICK RFU610-10610 with Firmware <2.25
- SICK RFU610-10613 with Firmware <2.25
- SICK RFU610-10614 with Firmware <2.25
- SICK RFU610-10618 with Firmware <2.25
- SICK RFU610-10700 with Firmware <2.25

Vendor Fix for CVE-2022-46832

Details: The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.

Valid for:

- SICK RFU620-10100 with Firmware <2.21
- SICK RFU620-10101 with Firmware <2.21
- SICK RFU620-10102 with Firmware <2.21
- SICK RFU620-10103 with Firmware <2.21
- SICK RFU620-10104 with Firmware <2.21
- SICK RFU620-10105 with Firmware <2.21
- SICK RFU620-10107 with Firmware <2.21
- SICK RFU620-10108 with Firmware <2.21
- SICK RFU620-10111 with Firmware <2.21
- SICK RFU620-10114 with Firmware <2.21
- SICK RFU620-10118 with Firmware <2.21
- SICK RFU620-10400 with Firmware <2.21
- SICK RFU620-10401 with Firmware <2.21
- SICK RFU620-10500 with Firmware <2.21
- SICK RFU620-10501 with Firmware <2.21
- SICK RFU620-10503 with Firmware <2.21
- SICK RFU620-10504 with Firmware <2.21
- SICK RFU620-10505 with Firmware <2.21
- SICK RFU620-10507 with Firmware <2.21
- SICK RFU620-10508 with Firmware <2.21
- SICK RFU620-10510 with Firmware <2.21
- SICK RFU620-10514 with Firmware <2.21

Vendor Fix for CVE-2022-46833

Details: The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.

Valid for:

- SICK RFU630-04100 with Firmware <2.21
- SICK RFU630-04100S01 with Firmware <2.21
- SICK RFU630-04101 with Firmware <2.21
- SICK RFU630-04102 with Firmware <2.21
- SICK RFU630-04103 with Firmware <2.21
- SICK RFU630-04104 with Firmware <2.21
- SICK RFU630-04105 with Firmware <2.21
- SICK RFU630-04106 with Firmware <2.21
- SICK RFU630-04108 with Firmware <2.21
- SICK RFU630-04109 with Firmware <2.21
- SICK RFU630-04117 with Firmware <2.21
- SICK RFU630-13100 with Firmware <2.21
- SICK RFU630-13100S01 with Firmware <2.21
- SICK RFU630-13101 with Firmware <2.21
- SICK RFU630-13102 with Firmware <2.21
- SICK RFU630-13103 with Firmware <2.21
- SICK RFU630-13104 with Firmware <2.21
- SICK RFU630-13105 with Firmware <2.21
- SICK RFU630-13106 with Firmware <2.21
- SICK RFU630-13107 with Firmware <2.21
- SICK RFU630-13108 with Firmware <2.21
- SICK RFU630-13110 with Firmware <2.21
- SICK RFU630-13111 with Firmware <2.21
- SICK RFU630-13113 with Firmware <2.21
- SICK RFU630-13114 with Firmware <2.21
- SICK RFU630-13115 with Firmware <2.21

Vendor Fix for CVE-2022-46834

Details: The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.

Valid for:

- SICK RFU650-10100 with Firmware <2.21
- SICK RFU650-10101 with Firmware <2.21

- SICK RFU650-10102 with Firmware <2.21
- SICK RFU650-10103 with Firmware <2.21
- SICK RFU650-10104 with Firmware <2.21
- SICK RFU650-10105 with Firmware <2.21
- SICK RFU650-10106 with Firmware <2.21

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

History

Version	Release Date	Comment
1	2022-12-08	Initial release
2	2023-02-10	Updated Advisory (only visual changes)