SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Password recovery vulnerability affects multiple SICK SIMs

Document ID:	SCA-2022-0013
Publication Date:	2022-11-04
CVE Identifiers:	CVE-2022-27582, CVE-2022-27584, CVE-2022-47377, CVE-2022-27585, CVE-2022-43989, CVE-2022-43990, CVE-2022-27586
Version:	3

Summary

SICK received a report about a vulnerability in multiple SICK SIM products. The vulnerability is classified as a ”Missing Authentication for Critical Function” vulnerability and results from a mishandling of access to a password recovery mechanism. It is possible for an unprivileged, remote user to invocate the password recovery mechanism without the needed authentication rights to gain access to the user-level ”RecoverableUserLevel” and thereby increasing their privileges on the system.

List of Products

Product	Part Number	Affected by
SIM1000 FX with Firmware <1.6.0	1097816 1097817	CVE-2022-27585 Status: Fixed Remediation: Vendor fix
SIM1004 with Firmware <2.0.0	1098148	CVE-2022-27586 Status: Fixed Remediation: Vendor fix
SIM1012 with Firmware <2.2.0	1098146	CVE-2022-43990 Status: Fixed Remediation: Vendor fix
SIM2000ST (LFT, PPC) with Firmware <1.13.4	2086502	CVE-2022-47377 Status: Fixed Remediation: Vendor fix

SIM2000ST (PPC) all Firmware versions	1080579	CVE-2022-27584 Status: Known Affected Remediation: Workaround
SIM2x00 (ARM) with Firmware <1.2.0	1092673 1081902	CVE-2022-43989 Status: Fixed Remediation: Vendor fix
SIM4000 (PPC) all Firmware versions	1078787	CVE-2022-27582 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2022-27582 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The firmware versions <=1.10.1 allow to optionally disable device configuration over the network interfaces. Please make sure that you apply general security practices when operating the SIM4000. A fix is planned but not yet scheduled.

CVE-2022-27582 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-306 (Missing Authentication for Critical Function)

CVE-2022-27584 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM2000ST Partnumber 1080579 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The firmware versions <=1.7.0 allow to optionally disable device configuration over the network interfaces. Please make sure that you apply general security practices when operating the SIM2000ST. A fix is planned but not yet scheduled.

CVE-2022-27584 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-306 (Missing Authentication for Critical Function)

CVE-2022-47377 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 with firmware version <1.13.4 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.13.4 as soon as possible (available in SICK Support Portal).

CVE-2022-47377 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-306 (Missing Authentication for Critical Function)

CVE-2022-27585 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM1000 FX Partnumber 1097816 and 1097817 with firmware version <1.6.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.6.0 as soon as possible (available in SICK Support Portal).

CVE-2022-27585 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-306 (Missing Authentication for Critical Function)

CVE-2022-43989 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber 1092673 and 1081902 with firmware version < 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.2.0 as soon as possible (available in SICK Support Portal).

CVE-2022-43989 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-306 (Missing Authentication for Critical Function)

CVE-2022-43990 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM1012 Partnumber 1098146 with firmware version <2.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 2.2.0 as soon as possible (available in SICK Support Portal).

CVE-2022-43990 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-306 (Missing Authentication for Critical Function)

CVE-2022-27586 Missing Authentication for Critical Function

Description: Password recovery vulnerability in SICK SIM1004 Partnumber 1098148 with firmware version <2.0.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 2.0.0 as soon as possible (available in SICK Support Portal).

CVE-2022-27586 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-306 (Missing Authentication for Critical Function)

Remediations

Workaround for CVE-2022-27582

Details: Please make sure that you apply general security practices when operating the SIM4000 (PPC). The firmware versions <=1.10.1 for SIM4000 allow to optionally disable device configuration over the network interfaces. Additionally, the following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled.

Valid for:

- SIM4000 (PPC) all Firmware versions

Workaround for CVE-2022-27584

Details: Please make sure that you apply general security practices when operating the SIM2000ST (part number 1080579). The firmware versions <=1.7.0 for SIM2000ST (part number 1080579) allow to optionally disable device configuration over the network interfaces. Additionally, the following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled.

Valid for:

- SIM2000ST (PPC) all Firmware versions

Vendor Fix for CVE-2022-47377

Details: The recommended solution is to update the firmware to a version >= 1.13.4 as soon as possible. The current firmware allows already to optionally disable device configuration over desired networks interfaces, especially in critical infrastructures.

Valid for:

- SIM2000ST (LFT, PPC) with Firmware <1.13.4

Vendor Fix for CVE-2022-27585

Details: The recommended solution is to update the firmware to a version >= 1.6.0 as soon as possible (available in SICK Support Portal).

Valid for:

- SIM1000 FX with Firmware <1.6.0

Vendor Fix for CVE-2022-43989

Details: The recommended solution is to update the firmware to a version >= 1.2.0 as soon as possible.

Valid for:

- SIM2x00 (ARM) with Firmware <1.2.0

Vendor Fix for CVE-2022-43990

Details: The recommended solution is to update the firmware to a version >= 2.2.0 as soon as possible (available in SICK Support Portal).

Valid for:

- SIM1012 with Firmware <2.2.0

Vendor Fix for CVE-2022-27586

Details: The recommended solution is to update the firmware to a version >= 2.0.0 as soon as possible.

Valid for:

- SIM1004 with Firmware <2.0.0

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.
Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

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
1	2022-10-21	Initial release
2	2022-11-04	Updated CVE references
3	2022-12-14	Additional CVE included