SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

OpenSSL vulnerability affects multiple SICK SIMs

Document ID:	SCA-2022-0012
Publication Date:	2022-08-03
CVE Identifier:	CVE-2022-0778
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	V1.0

Summary

In March 2022, the OpenSSL development team disclosed a denial of service in versions ”3.0.0,” ”3.0.1,” ”1.1.1”-”1.1.1m” and ”1.0.2-1.0.2zc” of the OpenSSL library. Exploiting this vulnerability allows remote, unauthenticated attackers to cause an infinite loop. It is possible to trigger the infinite loop by creating a certificate that has invalid explicit curve parameters or when parsing created private keys, as they may contain explicit elliptic curve parameters. It may be possible to put the SIMs in a non-responsive state since 100% of the CPU resource is consumed by the infinite loop calculation. The listed SICK SIM products are currently operated with an OpenSSL version that is vulnerable to CVE-2022-0778. With that it could be possible to exploit the mentioned vulnerability if the SIM devices are connected to a network with untrusted devices. In that case an untrusted client may send a manipulated SSH-certificate to the SIM, which exploits the vulnerability in the OpenSSL library as described above when it comes to the certificate validation by the SIM product. Evaluation is undergoing.

Affected Products

Product	Firmware Version	Part Number	Affected by
SIM4000	<= 1.10.1	1078787 1078484 1084131	CVE-2022-0778 Status: Affected Remediation: None available (fix planned), Workaround
SIM2000ST	<= 1.7.0	1080579	CVE-2022-0778 Status: Affected Remediation: None available (fix planned), Workaround

SIM2x00	<1.2.0	1081902 1092673 1112341	CVE-2022-0778 Status: Fixed Remediation: Vendor fix
SIM2000-2 P Track & Trace	<1.7.0	1117588	CVE-2022-0778 Status: Fixed Remediation: Vendor fix
SIM2000ST Track & Trace (2086501)	<= 1.7.0	2086501	CVE-2022-0778 Status: Affected Remediation: None available, Workaround
SIM2000ST Track & Trace (2086502)	<= 1.13.2	2086502	CVE-2022-0778 Status: Affected Remediation: None available, Workaround
SIM2000ST-E	<1.7.0	1112345	CVE-2022-0778 Status: Fixed Remediation: Vendor fix
SIM1012	<= 2.0.6	1098146	CVE-2022-0778 Status: Affected Remediation: None available (fix planned), Workaround
SIM1004	<= 1.1.0	1098148	CVE-2022-0778 Status: Affected Remediation: None available (fix planned), Workaround
SIM1000 FX	<= 1.5.2	1097816 1097817	CVE-2022-0778 Status: Affected Remediation: None available (fix planned), Workaround

Vulnerability Overview

CVE-2022-0778 Loop with Unreachable Exit Condition ('Infinite Loop')

Description of the original advisory from OpenSSL: „The OpenSSL BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial-of-service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters."

CVE-2022-0778 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5

CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
OpenSSL Security Advisory: https://www.openssl.org/news/secadv/20220315.txt
CVE Entry: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778

Remediations

None available for CVE-2022-0778

Valid for: SIM4000

Details: The recommended solution will be the update of the firmware to a version >= 1.10.2 (release not yet scheduled). Please see „Workaround“.

Vendor Fix for CVE-2022-0778

Valid for: SIM2x00

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

Vendor Fix for CVE-2022-0778

Valid for: SIM2000ST-E, SIM2000-2 P Track & Trace

Details: The recommended solution is to update the firmware to a version >= 1.7.0 as soon as possible.

None available for CVE-2022-0778

Valid for: SIM2000ST, SIM2000ST Track & Trace (2086501)

Details: The recommended solution will be the update of the firmware to a version >= 1.7.1 (release not yet scheduled). Please see „Workaround“.

None available for CVE-2022-0778

Valid for: SIM2000ST Track & Trace (2086502)

Details: The recommended solution will be the update of the firmware to a version >= 1.13.3 (release not yet scheduled).

None available for CVE-2022-0778

Valid for: SIM1012

Details: The recommended solution will be the update of the firmware to a version >= 2.1.0 (in progress, release not yet scheduled).

None available for CVE-2022-0778

Valid for: SIM1004

Details: The recommended solution will be the update of the firmware to a version >= 2.0.0 (in progress, release not yet scheduled).

None available for CVE-2022-0778

Valid for: SIM1000 FX

Details: The recommended solution will be the update of the firmware to a version >= 1.6.0 (in progress, release not yet scheduled).

Workaround for CVE-2022-0778

Valid for: SIM4000, SIM2000ST, SIM2000ST Track & Trace (2086501), SIM2000ST Track & Trace (2086502), SIM1012, SIM1004, SIM1000 FX

Details: In the runtime context of an SIM application, the SSH access should not be required at all, it is recommended as a workaround to disable port 22 (SSH) of the corresponding Ethernet port at the SIM via App (Firewall-API).

General Security Practices

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

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

Product Glossary

SIM4000	The programmable SIM4000 Sensor Integration Machine is opening up new possibilities for application solutions. Data from SICK sensors such as laser scanners and cameras can be merged into a point cloud, evaluated, archived, and transmitted. 8 Gigabit Ethernet interfaces are available for 2D or 3D cameras, and in some cases feature a voltage supply over Ethernet (PoE). Other sensors can be integrated via IO-Link, for example for distance and height measuring purposes.
SIM2000ST	The programmable Sensor Integration Machine SIM2000ST is opening up new possibilities for customized application solutions. Data from SICK sensors such as 1D/2D code sensors can be imported, evaluated, archived, and transmitted. In order to do this, the sensors can be connected to the SIM via the CAN bus. Ethernet-based fieldbus interfaces ensure rapid communication with controls.
SIM2x00	The programmable Sensor Integration Machines SIM2000 and SIM2500 offer multiple sensor data/camera acquisition and fusion processes, thereby providing space for new application solutions. The acquired data is processed and visualized for important information, for example quality control or process analysis. In addition, the IoT gateway functions enable connection from the edge to the cloud via the Internet in the context of Industry 4.0. The SIM2x00 products feature a powerful processor architecture and four fast Ethernet interfaces for cameras and LiDAR sensors. Other sensors can be integrated via IO-Link, for example for distance and height measuring purposes.
SIM2000-2 P Track & Trace	The pre-configured Sensor Integration Machine SIM2000-2 P is exclusively available for SICK track and trace systems of prime level.
SIM2000ST Track & Trace (2086501)	The pre-configured Sensor Integration Machines SIM2000ST (2086501 & 2086502) are exclusively available for SICK track and trace systems.
SIM2000ST Track & Trace (2086502)	The pre-configured Sensor Integration Machines SIM2000ST (2086501 & 2086502) are exclusively available for SICK track and trace systems.
SIM2000ST-E	The programmable SIM2000ST-E Sensor Integration Machine is opening up new possibilities for application solutions. Data from SICK sensors such as 1D / 2D code sensors can be imported, evaluated, archived, and transmitted. Four fast Ethernet interfaces are available for sensors. In addition, data from SICK LiDAR scanners can be read, merged into a point cloud, evaluated, archived, and transmitted.

SIM1012	The programmable SIM1012 Sensor Integration Machine is opening up new possibilities for application solutions. Data from SICK sensors such as laser scanners or cameras can be evaluated, archived, and transmitted. Sensors can be integrated via IO Link, for example for distance or height measurement. Ethernet interfaces with OPC-UA and MQTT provide pre-processed data (edge computing) for cloud computing. In addition, the SIM can be integrated into a SICK CAN sensor network.
SIM1004	The programmable Sensor Integration Machine SIM1004 is opening up new possibilities for application solutions. Data from SICK sensors such as laser scanners or cameras can be evaluated, archived, and transmitted. Sensors can be integrated via IO-Link, e. g. for distance and height measurement. Ethernet interfaces with OPC-UA and MQTT provide pre-processed data (edge computing) for cloud computing.
SIM1000 FX	The programmable Sensor Integration Machines SIM1000 FXA/FXG are opening up new possibilities for application solutions. It can read, evaluate, archive, and transmit data from a number of different sensors. The Ethernet interfaces with OPC UA and MQTT provide preprocessed data (edge computing) for cloud computing. The HMI and data visualization features can be provided on any browser-enabled notebook, PC, or tablet.

History

Version	Release Date	Comment
V1.0	2022-08-08	Initial Release