SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK Package Analytics

Document ID:	SCA-2022-0011
Publication Date:	2022-06-08
CVE Identifiers:	CVE-2021-3711, CVE-2021-35604, CVE-2021-22926
Version:	2

Summary

SICK received a report about multiple vulnerabilities in the SICK Package Analytics. The vulnerabilities result from the used MySQL database with version 5.7.25. The vulnerable MySQL version include Buffer-Overflow, Improper Access Control, and Improper Certification Validation vulnerabilities.
SICK has released a new version of the SICK Package Analytics and recommends updating to the newest version.

List of Products

Product	Affected by
SICK Package Analytics <4.4	CVE-2021-3711 Status: Known Affected Remediation: Vendor fix
	CVE-2021-35604 Status: Known Affected Remediation: Vendor fix
	CVE-2021-22926 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2021-3711 Stack-based Buffer Overflow

Description: A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behavior, or causing the application to crash.

CVE-2021-3711 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-121 (Stack-based Buffer Overflow)

CVE-2021-35604 Improper Access Control

Description: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data.

CVE-2021-35604 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H
CWE identifier: CWE-284 (Improper Access Control)

CVE-2021-22926 Improper Certificate Validation

Description: When libcurl is built to use the macOS native TLS library Secure Transport, an application can ask for the client certificate by name or with a file name - using the same option. If the name exists as a file, it will be used instead of by name. If the application runs with a current working directory that is writable by other users (like /tmp), a malicious user can create a file name with the same name as the app wants to use by name, and thereby trick the application to use the file based cert instead of the one referred to by name making libcurl send the wrong client certificate in the TLS connection handshake.

CVE-2021-22926 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
CWE identifier: CWE-295 (Improper Certificate Validation)

Remediations

Vendor Fix for CVE-2021-3711

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

Valid for:

- SICK Package Analytics <4.4

Vendor Fix for CVE-2021-35604

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

Valid for:

- SICK Package Analytics <4.4

Vendor Fix for CVE-2021-22926

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

Valid for:

- SICK Package Analytics <4.4

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 Package Analytics <4.4	Product on sick.com: https://www.sick.com/de/de/p/p600146

History

Version	Release Date	Comment
1	2022-06-08	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)