TLP:WHITE

SICK PSIRT
Security Advisory

Third party vulnerabilities in SICK CDE-100

Document ID:	SCA-2024-0004
Publication Date:	2024-11-07
CVE Identifiers:	CVE-2021-31571, CVE-2021-31572, CVE-2021-32020, CVE-2021-43997, CVE-2021-27504, CVE-2020-22284, CVE-2020-22283, CVE-2021-3399, CVE-2021-3890, CVE-2024-32883
Version:	2

Summary

The SICK CDE-100 uses the open-source libraries FreeRTOS, lwIP and MCU Boot. The used libraries contain vulnerabilities that affect the SICK CDE-100.

List of Products

Product	Part Number	Affected by
SICK CDE-100 all Firmware versions	1134028	CVE-2021-31571 Status: Under Investigation Remediation: Workaround
		CVE-2021-31572 Status: Under Investigation Remediation: Workaround
		CVE-2021-32020 Status: Under Investigation Remediation: Workaround
		CVE-2021-43997 Status: Known Not Affected Remediation: -

		CVE-2021-27504 Status: Known Not Affected Remediation: -
		CVE-2020-22284 Status: Known Not Affected Remediation: -
		CVE-2020-22283 Status: Known Not Affected Remediation: -
		CVE-2021-3399 Status: Known Not Affected Remediation: -
		CVE-2021-3890 Status: Under Investigation Remediation: Workaround
		CVE-2024-32883 Status: Under Investigation Remediation: Workaround

Vulnerability Overview

CVE-2021-31571 Integer Overflow or Wraparound

Summary: The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in queue.c for queue creation.

CVE-2021-31571 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-190 (Integer Overflow or Wraparound)

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2021-31571

CVE-2021-31572 Integer Overflow or Wraparound

Summary: The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer.

CVE-2021-31572 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-190 (Integer Overflow or Wraparound)

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2021-31572

CVE-2021-32020 Improper Restriction of Operations within the Bounds of a Memory Buffer

Summary: The kernel in Amazon Web Services FreeRTOS before 10.4.3 has insufficient bounds checking during management of heap memory.

CVE-2021-32020 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-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2021-32020

CVE-2021-43997 Improper Privilege Management

Summary: FreeRTOS versions 10.2.0 through 10.4.5 do not prevent non-kernel code from calling the xPortRaisePrivilege internal function to raise privilege. FreeRTOS versions through 10.4.6 do not prevent a third party that has already independently gained the ability to execute injected code to achieve further privilege escalation by branching directly inside a FreeRTOS MPU API wrapper function with a manually crafted stack frame. These issues affect ARMv7-M MPU ports, and ARMv8-M ports with MPU support enabled (i.e. configENABLE_MPU set to 1). These are fixed in V10.5.0 and in V10.4.3-LTS Patch 3.

CVE-2021-43997 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-269 (Improper Privilege Management)

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2021-43997

CVE-2021-27504 Integer Overflow or Wraparound

Summary: Texas Instruments devices running FREERTOS, malloc returns a valid pointer to a small buffer on extremely large values, which can trigger an integer overflow vulnerability in 'malloc' for FreeRTOS, resulting in code execution.

CVE-2021-27504 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-190 (Integer Overflow or Wraparound)

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2021-27504

CVE-2020-22284 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Summary: A buffer overflow vulnerability in the zepif_linkoutput() function of Free Software Foundation lwIP git head version and version 2.1.2 allows attackers to access sensitive information via a crafted 6LoWPAN packet.

CVE-2020-22284 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:H/I:N/A:N
CWE identifier: CWE-120 (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))

References:
NVD Entry:
https://nvd.nist.gov/vuln/detail/CVE-2020-22284

CVE-2020-22283 Excessive Code Complexity

Summary: A buffer overflow vulnerability in the icmp6_send_response_with_addrs_and_netif() function of Free Software Foundation lwIP version git head allows attackers to access sensitive information via a crafted ICMPv6 packet.

CVE-2020-22283 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:H/I:N/A:N
CWE identifier: CWE-1120 (Excessive Code Complexity)

CVE-2021-3399 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Summary: The MCUboot project uses hard-coded public/private keys as an aid to developers. Although documented that anyone producing a product using MCUboot should create their own keys, the build system does not encourage this, and it is very easy to produce a product using these keys.

CVE-2021-3399 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.6
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-1321 (Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'))

References:
GitHub Entry:
https://github.com/mcu-tools/mcuboot/security/advisories/GHSA-gcxh-546h-phg4

CVE-2021-3890 Integer Overflow to Buffer Overflow

Summary: In case MCUBOOT_MEASURED_BOOT is defined the TLV structure is parsed in order to retrieve the information from the image in flash and use it for saving the status information.
Two TLV fields are retrieved by the mcuboot, namely IMAGE_TLV_BOOT_RECORD and IMAGE_TLV_SHA256.
Since the length of the TLV field is defined by the TLV itself it is possible that length record_len in IMAGE_TLV_BOOT_RECORD is reasonably arbitrary.
The TLV data in the image stored in flash cannot be fully trusted since there is no authentication of the TLV data performed by the mcuboot bootloader. In case of an external SPI flash the tlv data can be easily modified by the attacker as well.
The value record_len is checked to be not larger than the receiving buffer buf, but not checked if it is smaller than the expected length.
In case record_len is smaller than sizeof(image_hash) integer underflow will take place resulting in a negative value interpreted as an unsigned value. Once the offset is added to the pointer buff the destination pointer value will overflow and up to 31 bytes of attacker controlled data will be written on the stack out of bounds, resulting in the stack memory corruption and depending on the stack layout can lead to an arbitrary code execution.

CVE-2021-3890 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.8
CVSSv3.1 vector string: CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
CWE identifier: CWE-680 (Integer Overflow to Buffer Overflow)

References:
GitHub Entry:
https://github.com/mcu-tools/mcuboot/security/advisories/GHSA-8hrv-4cp5-4rg3

CVE-2024-32883 Improper Validation of Integrity Check Value

Summary: MCUboot uses a TLV (tag-length-value) structure to represent the meta data associated with an image. The TLVs themselves are divided into two sections, a protected and an unprotected section. The protected TLV entries are included as part of the image signature to avoid tampering. However, the code does not distinguish which TLV entries should be protected or not, so it is possible for an attacker to add unprotected TLV entries that should be protected. Currently, the primary protected TLV entries should be the dependency indication, and the boot record. An injected dependency value would primarily result in an otherwise acceptable image being rejected. A boot record injection could allow fields in a later attestation record to include data not intended, which could cause an image to appear to have properties that it should not have.

CVE-2024-32883 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.7
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:H
CWE identifier: CWE-354 (Improper Validation of Integrity Check Value)

References:
GitHub Entry:
https://github.com/mcu-tools/mcuboot/security/advisories/GHSA-m59c-q9gq-rh2j

Remediations

Workaround for CVE-2021-31571

Details: SICK is still investigating if the CDE-100 is affected by this vulnerability.
Please make sure that you apply general security practices when operating the CDE-100 like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK CDE-100 all Firmware versions

Workaround for CVE-2021-31572

Details: SICK is still investigating if the CDE-100 is affected by this vulnerability.
Please make sure that you apply general security practices when operating the CDE-100 like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK CDE-100 all Firmware versions

Workaround for CVE-2021-32020

Details: SICK is still investigating if the CDE-100 is affected by this vulnerability.
Please make sure that you apply general security practices when operating the CDE-100 like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK CDE-100 all Firmware versions

Workaround for CVE-2021-3890

Details: SICK is currently investigating whether the CDE-100 is impacted by this vulnerability.
Please make sure that you apply general security practices when operating the CDE-100 like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK CDE-100 all Firmware versions

Workaround for CVE-2024-32883

Details: SICK is currently investigating whether the CDE-100 is impacted by this vulnerability.
Please make sure that you apply general security practices when operating the CDE-100 like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK CDE-100 all Firmware versions

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:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2024-11-07	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated