



Sensor Intelligence.

TLP:WHITE

SICK PSIRT Security Advisory

FreeRTOS Vulnerabilities have no impact on SICK Products

Document ID: SCA-2025-0003
Publication Date: 2026-04-17
CVE Identifiers: CVE-2024-28115, CVE-2018-16525, CVE-2021-43997, CVE-2021-31571, CVE-2021-32020, CVE-2021-31572, CVE-2018-16601, CVE-2018-16526, CVE-2018-16523, CVE-2018-16600, CVE-2018-16527, CVE-2018-16524, CVE-2018-16599, CVE-2018-16598, CVE-2018-16602, CVE-2018-16603
Version: 4

Summary

FreeRTOS has several known vulnerabilities and is used in various SICK products. A current analysis confirms that the identified vulnerabilities in FreeRTOS do not affect the mentioned SICK products. At this time, there is no indication of any potential risks to these SICK products.

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

List of Products

Product	Part Number	Affected by
SICK ANM58B all Firmware versions	1145910	CVE-2024-28115 Status: Known Not Affected Remediation: -
	1146128	
	1146129	
	1146130	
	1146132	
	1146133	
	1146134	
	1146135	
	1146136	
	1146137	
	1146519	
	1146524	
	1146526	
	1146529	
	1146643	
	1146644	
	1146645	
	1146648	
	1148701	
	1148703	
1148711		
1148725		
1148730		
		CVE-2018-16525 Status: Known Not Affected Remediation: -
		CVE-2021-43997 Status: Known Not Affected Remediation: -
		CVE-2021-31571 Status: Known Not Affected Remediation: -
		CVE-2021-32020 Status: Known Not Affected Remediation: -
		CVE-2021-31572 Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

	<p>CVE-2018-16601 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

SICK ANS58B all Firmware versions	1145911	CVE-2024-28115
	1145966	Status: Known Not Affected
	1146127	Remediation: -
	1146131	
	1146525	
	1146658	
	1148702	
	1148706	
	1148712	
	1148713	
	1148717	
	1148718	
	1148721	
	1148722	
1148726		
1148727		
1148731		
1148732		
1149238		
1149416		
1149417		
1149418		
		CVE-2018-16525
		Status: Known Not Affected
		Remediation: -
		CVE-2021-43997
		Status: Known Not Affected
		Remediation: -
		CVE-2021-31571
		Status: Known Not Affected
		Remediation: -
		CVE-2021-32020
		Status: Known Not Affected
		Remediation: -
		CVE-2021-31572
		Status: Known Not Affected
		Remediation: -
		CVE-2018-16601
		Status: Known Not Affected
		Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK DCM4 with Firmware 1.2.0 up to 1.4.0	1125888	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		CVE-2021-32020 Status: Known Not Affected Remediation: -
		CVE-2021-31572 Status: Known Not Affected Remediation: -
		CVE-2018-16601 Status: Known Not Affected Remediation: -
		CVE-2018-16526 Status: Known Not Affected Remediation: -
		CVE-2018-16523 Status: Known Not Affected Remediation: -
		CVE-2018-16600 Status: Known Not Affected Remediation: -
		CVE-2018-16527 Status: Known Not Affected Remediation: -
		CVE-2018-16524 Status: Known Not Affected Remediation: -
		CVE-2018-16599 Status: Known Not Affected Remediation: -
		CVE-2018-16598 Status: Known Not Affected Remediation: -
		CVE-2018-16602 Status: Known Not Affected Remediation: -
		CVE-2018-16603 Status: Known Not Affected Remediation: -
SICK DMM4 with Firmware 1.2.0 up to 1.4.0	1125562	CVE-2024-28115 Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

<u>CVE-2018-16525</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-43997</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31571</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16526</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16523</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16600</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16527</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16524</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16599</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16598</u> Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<u>CVE-2018-16602</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16603</u> Status: Known Not Affected Remediation: -
SICK FXL1 with Firmware 1.6.0 up to 1.21.0	1101320 1101321 1101322 1101323 1101324 1101325 1120827 1120828 1122586 1122587 1112205 1112206 1143315 1143316 1144849 1144850	<u>CVE-2024-28115</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16525</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-43997</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-31571</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK SE1 with Firmware 1.16.0 up to 1.17.0	1132196 1132197	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

	<p><u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16526</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16523</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16600</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16527</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16524</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16599</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16598</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16602</u> Status: Known Not Affected Remediation: -</p>
	<p><u>CVE-2018-16603</u> Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

**SICK deTec4 with Firmware
1.05 up to 1.51.0**

- 1116161
- 1116162
- 1116163
- 1116164
- 1116165
- 1116166
- 1116167
- 1220084
- 1220085
- 1220086
- 1220087
- 1220088
- 1220089
- 1220090
- 1220091
- 1220092
- 1220093
- 1220094
- 1220095
- 1220096
- 1220097
- 1220098
- 1220099
- 1220100
- 1220101
- 1220102
- 1220103
- 1220104
- 1220105
- 1220106
- 1220107
- 1220108
- 1220109
- 1220110
- 1220111
- 1220112
- 1220113
- 1220114
- 1220115
- 1220116
- 1220117
- 1220118
- 1220119
- 1220120
- 1220121
- 1220122
- 1220123
- 1220124
- 1220125
- 1220126
- 1220127
- 1220128
- 1220129
- 1220130
- 1220131

CVE-2024-28115

Status: Known Not Affected

Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

<u>CVE-2018-16525</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-43997</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31571</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16526</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16523</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16600</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16527</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16524</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16599</u> Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK deTem2 Core A/P with Firmware 1.04 up to 1.10	1101921 1102144 1102646 1102647 1103066 1103067	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-32020 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31572 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16601 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK deTem4 A/P with Firmware 1.02 up to 1.32.0	1101921 1102144 1102633 1102634 1102635 1102636 1103066 1103067	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p> <p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

	<p>CVE-2021-32020 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2021-31572 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16601 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p>
	<p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

SICK deTem4 Core A/P with Firmware 1.04 up to 1.10	1101921	CVE-2024-28115
	1102144	Status: Known Not Affected
	1102644	Remediation: -
	1102645	
	1103066	
	1103067	
		CVE-2018-16525
		Status: Known Not Affected
		Remediation: -
		CVE-2021-43997
		Status: Known Not Affected
		Remediation: -
		CVE-2021-31571
	Status: Known Not Affected	
	Remediation: -	
	CVE-2021-32020	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2021-31572	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16601	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16526	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16523	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16600	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16527	
	Status: Known Not Affected	
	Remediation: -	
	CVE-2018-16524	
	Status: Known Not Affected	
	Remediation: -	

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK deTem4 LT Muting A/P with Firmware 1.10	1110584 1108692 1108691	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-32020 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31572 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16601 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16600 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16527 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16524 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
<p>SICK deTem4 with Firmware 1.02 up to 1.3.0</p>	<p>1128426 1128427 1128428 1128429 1128430 1128431 1128432 1128433 1128434 1128435 1128436 1128437 1128438 1128439 1128440</p>	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p> <p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

<u>CVE-2021-43997</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31571</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -
<u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16526</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16523</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16600</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16527</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16524</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16599</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16598</u> Status: Known Not Affected Remediation: -
<u>CVE-2018-16602</u> Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<u>CVE-2018-16603</u> Status: Known Not Affected Remediation: -
SICK safeVisionary2 all Firmware versions	1116398	<u>CVE-2024-28115</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16525</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-43997</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-31571</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-32020</u> Status: Known Not Affected Remediation: -
		<u>CVE-2021-31572</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16601</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16526</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16523</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16600</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16527</u> Status: Known Not Affected Remediation: -
		<u>CVE-2018-16524</u> Status: Known Not Affected Remediation: -

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

		<p>CVE-2018-16599 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16598 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16602 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16603 Status: Known Not Affected Remediation: -</p>
SICK scanGrid2 with Firmware 1.10 up to 1.15	1101561 1109414	<p>CVE-2024-28115 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16525 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-43997 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31571 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-32020 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2021-31572 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16601 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16526 Status: Known Not Affected Remediation: -</p>
		<p>CVE-2018-16523 Status: Known Not Affected Remediation: -</p>

TLP:WHITE



Sensor Intelligence.

TLP:WHITE

	CVE-2018-16600 Status: Known Not Affected Remediation: -
	CVE-2018-16527 Status: Known Not Affected Remediation: -
	CVE-2018-16524 Status: Known Not Affected Remediation: -
	CVE-2018-16599 Status: Known Not Affected Remediation: -
	CVE-2018-16598 Status: Known Not Affected Remediation: -
	CVE-2018-16602 Status: Known Not Affected Remediation: -
	CVE-2018-16603 Status: Known Not Affected Remediation: -

Vulnerability Overview

CVE-2024-28115 Improper Handling of Insufficient Permissions or Privileges

Summary: FreeRTOS is a real-time operating system for microcontrollers. FreeRTOS Kernel versions through 10.6.1 do not sufficiently protect against local privilege escalation via Return Oriented Programming techniques should a vulnerability exist that allows code injection and execution. These issues affect ARMv7-M MPU ports, and ARMv8-M ports with Memory Protected Unit (MPU) support enabled (i.e. configENABLE_MPU set to 1). These issues are fixed in version 10.6.2 with a new MPU wrapper.

CVE-2024-28115 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-280 (Improper Handling of Insufficient Permissions or Privileges)

TLP:WHITE

CVE-2018-16525

Summary: Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow remote attackers to execute arbitrary code or leak information because of a Buffer Overflow during parsing of DNS\LLMNR packets in prvParseDNSReply.

CVE-2018-16525 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.1

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

CVE-2021-43997

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

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)

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)

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)

CVE-2018-16601 Integer Underflow (Wrap or Wraparound)

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. A crafted IP header triggers a full memory space copy in prvProcessIPPacket, leading to denial of service and possibly remote code execution.

CVE-2018-16601 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.1

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

CWE identifier: CWE-191 (Integer Underflow (Wrap or Wraparound))

CVE-2018-16526

Summary: Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow remote attackers to leak information or execute arbitrary code because of a Buffer Overflow during generation of a protocol checksum in usGenerateProtocolChecksum and prvProcessIPPacket.

CVE-2018-16526 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.1

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

CVE-2018-16523 Divide By Zero

Summary: Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow division by zero in prvCheckOptions.

CVE-2018-16523 has been assigned to this vulnerability.

CVSSv3.1 base score: 7.4

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

CWE identifier: CWE-369 (Divide By Zero)

CVE-2018-16600 Exposure of Sensitive Information to an Unauthorized Actor

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of ARP packets in eARPPProcessPacket can be used for information disclosure.

CVE-2018-16600 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2018-16527 Exposure of Sensitive Information to an Unauthorized Actor

Summary: Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow information disclosure during parsing of ICMP packets in prvProcessICMPPacket.

CVE-2018-16527 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2018-16524 Exposure of Sensitive Information to an Unauthorized Actor

Summary: Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow information disclosure during parsing of TCP options in prvCheckOptions.

CVE-2018-16524 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2018-16599 Exposure of Sensitive Information to an Unauthorized Actor

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of NBNS packets in prvTreatNBNS can be used for information disclosure.

CVE-2018-16599 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2018-16598 Unintended Proxy or Intermediary ('Confused Deputy')

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. In xProcessReceivedUDPPacket and prvParseDNSReply, any received DNS response is accepted, without confirming it matches a sent DNS request.

CVE-2018-16598 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-441 (Unintended Proxy or Intermediary ('Confused Deputy'))

CVE-2018-16602 Exposure of Sensitive Information to an Unauthorized Actor

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of DHCP responses in prvProcessDHCPReplies can be used for information disclosure.

CVE-2018-16602 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2018-16603 Exposure of Sensitive Information to an Unauthorized Actor

Summary: An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds access to TCP source and destination port fields in xProcessReceivedTCPPacket can leak data back to an attacker.

CVE-2018-16603 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9

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

CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

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	2025-02-28	Initial version
2	2025-05-20	Added two products: ANS58 and ANM58. Both have the product status 'Known Not Affected'.
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated
4	2026-04-17	Added product: DCM4 (status: known not affected) and adjusted version ranges for: DMM4, deTec4, deTem4, deTem4 A/P (all versions marked as known not affected)