SICK Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Gateways for Flexi Soft, Flexi Compact, SICK EFI Gateway UE4740, SICK microScan3 and outdoorScan3

Document ID:	SCA-2022-0008
Publication Date:	2022-04-29
CVE Identifier:	N/A (CWE-400)
CVSSv3 Base Score:	6.5
CVSSv3 Vector String:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	3

Summary

The PSIRT received a report about a vulnerability in some gateways for Flexi Soft, Flexi Compact, EFI gateway UE4740, microScan3 and the outdoorScan3. The vulnerability is classified as a denial-of-service vulnerability and results from a malformed UDP package. It is recommended to implement the mitigations described in the mitigations section.

List of Products

Product	Part Number	Affected by
SICK FLX0-GPNT1 with Firmware 1.01.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK FX0-GENT with Firmware 3.04.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK FX0-GENT with Firmware 3.05.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK FX0-GPNT with Firmware 3.04.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK FX0-GPNT with Firmware 3.05.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK FX3-GEPR with Firmware <=1.07.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1108231	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ40IZ1 with Firmware 1.14 up to 1.53	1075845	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.76	1100403	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ40ZA1 with Firmware 1.14 up to 1.53	1092539	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-ABAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1108233	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ55IZ1 with Firmware 1.14 up to 1.53	1075848	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.76	1100405	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ55ZA1 with Firmware 1.14 up to 1.53	1092538	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1108235	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ90IZ1 with Firmware 1.14 up to 1.53	1094456	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.76	1100407	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ90ZA1 with Firmware 1.14 up to 1.53	1094455	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.76	1100383	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.76	1083011	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.76	1100385	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.76	1083009	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.76	1100387	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.76	1094458	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1108227	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ40IZ1 with Firmware 1.14 up to 1.53	1092540	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.76	1092718	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ40ZA1 with Firmware 1.14 up to 1.53	1091037	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1104317	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ55IZ1 with Firmware 1.14 up to 1.53	1092541	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.76	1092718	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ55ZA1 with Firmware 1.14 up to 1.53	1091038	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled	1108229	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ90IZ1 with Firmware 1.14 up to 1.53	1094460	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.76	1094462	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ90ZA1 with Firmware 1.14 up to 1.53	1094465	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBUZ40IZ1 with Firmware 1.43	1094472	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ40AA1 with Firmware 1.14 up to 1.53	1110035	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.76	1100397	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.76	1100389	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ55AA1 with Firmware 1.14 up to 1.53	1110033	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.76	1100399	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.76	1100391	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ90AA1 with Firmware 1.14 up to 1.53	1110037	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.76	1100401	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.76	1100393	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK UE4740 EFI gateway all Firmware versions		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

Vulnerability Overview

Uncontrolled Resource Consumption

Summary: The vulnerability is classified as a denial-of-service vulnerability and results from a malformed UDP package. An attacker could use this vulnerability to affect the availability of the safety controllers Flexi Soft, Flexi Compact, EFI gateway UE4740 and the safety laser scanners mircoScan3 and outdoorScan3. Even if Flexi Soft, Flexi Compact, UE4740, microScan3 or outdoorScan3 are made unavailable, no safety issue ensues. The main module of the gateways set its outputs in the safe state (low). It is recommended to implement the mitigations described in the mitigations section.

No CVE has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

Impact: An attacker that has access to one of the above listed products with the corresponding firmware versions could affect the availability by exploiting the gateways or the devices with a malformed UDP header. This forces the main module of the gateways to set its outputs in the safe state (low).

Remediations

Mitigation for Uncontrolled Resource Consumption

Details: Please make sure that you apply general security practices when operating the FlexiSoft, FlexiCompact, UE4740 EFI gateway, mircoScan3 and outdoorScan3. The following general security practices could mitigate the associated security risk.

Valid for:

- SICK FLX0-GPNT1 with Firmware 1.01.0
- SICK FX0-GENT with Firmware 3.04.0
- SICK FX0-GENT with Firmware 3.05.0
- SICK FX0-GPNT with Firmware 3.04.0
- SICK FX0-GPNT with Firmware 3.05.0
- SICK FX3-GEPR with Firmware <=1.07.0
- SICK MICS3-ABAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ40IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ABAZ40ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ55IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ABAZ55ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ90IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ABAZ90ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ40IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.76

- SICK MICS3-CBAZ40ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ55IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ55ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ90IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ90ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBUZ40IZ1 with Firmware 1.43
- SICK MICS3-CCAZ40AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ55AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ90AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK UE4740 EFI gateway all Firmware versions

None available for Uncontrolled Resource Consumption

Details: Currently there is no remediation.

Valid for:

- SICK FLX0-GPNT1 with Firmware 1.01.0
- SICK FX0-GENT with Firmware 3.04.0
- SICK FX0-GENT with Firmware 3.05.0
- SICK FX0-GPNT with Firmware 3.04.0
- SICK FX0-GPNT with Firmware 3.05.0
- SICK FX3-GEPR with Firmware <=1.07.0
- SICK MICS3-ABAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ40IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ABAZ40ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ55IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.76

- SICK MICS3-ABAZ55ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-ABAZ90IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ABAZ90ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ40EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ40IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ40ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ55EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ55IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ55ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ90EN1 with Firmware 1.52 up to 1.76, if (Ethernet over EtherCAT) enabled
- SICK MICS3-CBAZ90IZ1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CBAZ90ZA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CBUZ40IZ1 with Firmware 1.43
- SICK MICS3-CCAZ40AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ55AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ90AA1 with Firmware 1.14 up to 1.53
- SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.76
- SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.76
- SICK UE4740 EFI gateway 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://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

History

Version	Release Date	Comment
1	2022-04-29	Initial Release
2	2022-06-20	Updated affected products
3	2023-02-10	Updated Advisory (only visual changes)