SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in Platform Mechanism AutoIP

Document ID:	SCA-2020-0004
Publication Date:	2020-08-31
CVE Identifier:	CVE-2020-2075
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:	3

Summary

SICK received a report from IOActive that informed SICK about a security vulnerability within the platform mechanism AutoIP, used by multiple devices.
SICK recommends updating to the newest version. Refer to the recommended remediations for affected products where no update is available.
Currently SICK is not aware of any public exploits specifically targeting this vulnerability.

List of Products

Product	Affected by
SICK Bulkscan LMS111 with Firmware <1.04	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK Bulkscan LMS511 with Firmware <2.3	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK CLV62x with Firmware <=6.10	CVE-2020-2075 Status: Known Affected Remediation: Workaround

SICK CLV63x with Firmware <=6.10	CVE-2020-2075 Status: Known Affected Remediation: Workaround
SICK CLV64x with Firmware <=6.10	CVE-2020-2075 Status: Known Affected Remediation: Workaround
SICK CLV65x with Firmware <=6.10	CVE-2020-2075 Status: Known Affected Remediation: Workaround
SICK ICR890-3 all Firmware versions	CVE-2020-2075 Status: Known Affected Remediation: Workaround
SICK LMS10x with Firmware <2.0	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS11x with Firmware <2.0	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS12x with Firmware <2.1	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS13x with Firmware <2.1	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS14x with Firmware <2.1	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS15x with Firmware <2.0	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK LMS53x all Firmware versions	CVE-2020-2075 Status: Known Affected Remediation: Workaround
SICK LMS5xx all Firmware versions	CVE-2020-2075 Status: Known Affected Remediation: Workaround

SICK MSC800 with Firmware <4.1	CVE-2020-2075 Status: Known Affected Remediation: Vendor fix
SICK RFH all Firmware versions	CVE-2020-2075 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2020-2075

Description: Improper handling of exceptional conditions in the platform mechanism AutoIP can lead to a reboot of the device, if parsing malformed network packets. This can lead to a temporary impact of the availability of the device. The AutoIP mechanism is used by the SOPAS Engineering Tool (SOPAS-ET), e.g. to detect SICK devices in the network and change their IP configuration. This is intended to simplify the initial setup and the maintenance of the devices. The devices listen on port 30718 for UDP broadcasts.
SICK has released a new firmware version for the MSC800, Bulkscan LMS111, Bulkscan LMS511 and other LMS1xx devices.

CVE-2020-2075 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

Remediations

Vendor Fix for CVE-2020-2075

Details: Update to version V1.04
SICK removed the AutoIP weakness with the same available fix for the MSC800. The update can only be implemented by a SICK service technician, either by remote access or on site. To obtain the update, please contact your local service technician.

Valid for:

- SICK Bulkscan LMS111 with Firmware <1.04

Details: Update to version V2.30
SICK removed the AutoIP weakness with the same available fix for the MSC800. The update can only be implemented by a SICK service technician, either by remote access or on site. To obtain the update, please contact your local service technician.

Valid for:

- SICK Bulkscan LMS511 with Firmware <2.3

Details: Update to version V2.0
The update fixes, that the LMS1xx series does not reboot anymore, after it received an incorrect payload on the AutoIP port. There are no known limitations. The update to version V2.0 respectively V2.10 will be available from mid-October 2020 on. To get the latest LMS1xx firmware update, please contact the responsible SICK Sales and Service unit, or download it from sick.com.

Valid for:

- SICK LMS10x with Firmware <2.0
- SICK LMS11x with Firmware <2.0
- SICK LMS15x with Firmware <2.0

Details: Update to version V2.10
The update fixes, that the LMS1xx series does not reboot anymore, after it received an incorrect payload on the AutoIP port. There are no known limitations. The update to version V2.0 respectively V2.10 will be available from mid-October 2020 on. To get the latest LMS1xx firmware update, please contact the responsible SICK Sales and Service unit, or download it from sick.com.

Valid for:

- SICK LMS12x with Firmware <2.1
- SICK LMS13x with Firmware <2.1
- SICK LMS14x with Firmware <2.1

Details: Update to version V4.1
The update fixes that the MSC800 does not reboot anymore after it received an incorrect payload on the AutoIP port. There are no known limitations. To get the latest MSC800 firmware update please contact the responsible SICK Sales and Service unit. They can support if there is the need to consider any customer specific changes or constraints related to legal for trade systems.

Valid for:

- SICK MSC800 with Firmware <4.1

Workaround for CVE-2020-2075

Details: Restrict or block access to UDP port 30718 for the affected products. This workaround reduces the risk of the exploitation of the vulnerability but also limits the AutoIP function.

Valid for:

- SICK CLV62x with Firmware <=6.10
- SICK CLV63x with Firmware <=6.10

- SICK CLV64x with Firmware <=6.10
- SICK CLV65x with Firmware <=6.10
- SICK ICR890-3 all Firmware versions
- SICK LMS53x all Firmware versions
- SICK LMS5xx all Firmware versions
- SICK RFH 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:
http://ics-cert.us-cert.gov/content/recommended-practices

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

Acknowledgments

Thanks to Ruben Santamarta from IOActive for his research and the report..

Additional Product Information

SICK CLV62x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv62x/c/g79824
SICK CLV63x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv63x/c/g79846
SICK CLV64x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv64x/c/g79874
SICK CLV65x with Firmware <=6.10	Product on sick.com: https://www.sick.com/de/de/identifikationsloesungen/stationaere-barcode-scanner/clv65x/c/g79879
SICK LMS5xx all Firmware versions	Product on sick.com: https://www.sick.com/de/de/lidar-sensoren/2d-lidar-sensoren/lms5xx/c/g179651

History

Version	Release Date	Comment
1	2020-10-29	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated