TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in platform mechanism AutoIP

Document ID:	SCA-2020-0004
Publication Date:	2020-08-31
CVSSv3 Base Score:	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE Identifier:	CVE-2020-2075
Version:	V1.0

SUMMARY

SICK received a report from IOActive that informed SICK about a security vulnerability within the platform mechanism AutoIP, used by multiple devices. Improper handling of exceptional conditions 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. SICK recommends updating to the newest version. Refer to the recommended actions from section “Workarounds and Mitigations” for affected products where no update is available

Currently SICK is not aware of any public exploits specifically targeting this vulnerability.

AFFECTED PRODUCTS

Product	Version	Remediation
Bulkscan LMS111	All Versions < V1.04	Update to version V1.04
Bulkscan LMS511	All Versions < V2.30	Update to version V2.30
CLV62x – CLV65x	All versions with Ethernet interface	Refer to recommended actions from section “Workarounds and Mitigations”
ICR890-3	All ICR890-3 and ICR890-3.5 devices all versions	Refer to recommended actions from section “Workarounds and Mitigations”
LMS10x, LMS11x, LMS15x	All Versions < V2.0	Update to version V2.0
LMS12x, LMS13x, LMS14x	All Versions < V2.10	Update to version V2.10
LMS5xx, LMS53x	All versions	Refer to recommended actions from section “Workarounds and Mitigations”
MSC800	all Versions < V4.10	Update to version V4.10
RFH	All versions	Refer to recommended actions from section “Workarounds and Mitigations”

Bulkscan LMS111 AND LMS511

SICK removed the AutoIP weakness with the same available fix for the MSC-800. 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.

LMS1xx

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.

MSC800

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.

WORKAROUNDS AND MITIGATIONS

SICK recommends the following measure for solutions where an update is not applicable or a technical fix is not available:

- 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.

GENERAL SECURITY RECOMMENDATIONS

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.

Additional information on Industrial Security can be found at:
https://sick.com/psirt

VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.0). 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.

ACKNOWLEDGMENTS

SICK thanks Ruben Santamarta, Principal Security Consultant at IOActive, for his research and the report.

RESOURCES

CVSS Calculator
https://www.first.org/cvss/calculator/3.0#

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

HISTORY

Version	Release Date	Comment
V1.0	2020-08-31	Initial Release