SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Incoming Goods Suite

Document ID:	SCA-2024-0005
Publication Date:	2024-11-19
CVE Identifier:	CVE-2024-11075
CVSSv3 Base Score:	8.8
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Version:	1

Summary

SICK found a vulnerability in the Incoming Goods Suite which allows privilege escalation to the administrative level. Currently SICK is not aware of any public exploits specifically targeting the vulnerability. SICK has released a new version and strongly recommends updating to the newest version.

List of Products

Product	Affected by
SICK Incoming Goods Suite 1.0.0	CVE-2024-11075 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2024-11075 Execution with Unnecessary Privileges

Summary: A vulnerability in the Incoming Goods Suite allows a user with unprivileged access to the underlying system (e.g. local or via SSH) a privilege escalation to the administrative level due to the usage of component vendor Docker images running with root permissions. Exploiting this misconfiguration leads to the fact that an attacker can gain administrative control over the whole system.

CVE-2024-11075 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-250 (Execution with Unnecessary Privileges)

Remediations

Vendor Fix for CVE-2024-11075

Details: Customers are strongly recommended to upgrade to the latest release 1.1.0. In addition, we recommend running the Docker daemon and container runtime in rootless mode. It is necessary to set the DOCKER_USER_ID and the DOCKER_GROUP_ID in the environment. Then the Docker socket can run as a non-root user when setting the path DOCKER_SOCKET_PATH=/run/user/${DOCKER_USER_ID}/docker.sock.

Valid for:

- SICK Incoming Goods Suite 1.0.0

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

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

Linux post-installation steps for Docker Engine.:
https://docs.docker.com/engine/install/linux-postinstall/

Docker rootless mode to execute the Docker daemon and containers inside a user namespace.:
https://docs.docker.com/engine/security/rootless/

History

Version	Release Date	Comment
1	2024-11-19	Initial version