TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability Affecting SICK Sentio Creator Extension „Software Deployment Manager“

Document ID:	SCA-2026-0008
Publication Date:	2026-07-10
CVE Identifier:	CVE-2026-33151
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:	1

Summary

The pre-installed Software Deployment Manager extension in SICK Sentio Creator is affected by CVE-2026-33151. The Software Deployment Manager extension is maintained and updated independently from SICK Sentio Creator and therefore SICK recommends applying the defined remediations for the vulnerability.

List of Products

Product	Affected by
SICK Sentio Creator all versions using Software Deployment Manager Version <0.14.0	CVE-2026-33151 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2026-33151 Improper Input Validation

Summary: Socket.IO is an open source, real-time, bidirectional, event-based, communication framework. Prior to versions 3.3.5, 3.4.4, and 4.2.6, a specially crafted Socket.IO packet can make the server wait for a large number of binary attachments and buffer them, which can be exploited to make the server run out of memory. This issue has been patched in versions 3.3.5, 3.4.4, and 4.2.6.

CVE-2026-33151 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
CWE identifier: CWE-20 (Improper Input Validation)

Remediations

Vendor Fix for CVE-2026-33151

Details: Users are strongly recommended to upgrade the Software Deployment Manager extension for Sentio Creator to version 0.14.0.

Valid for:

- SICK Sentio Creator all versions using Software Deployment Manager Version $<$0.14.0

General Security Practices

General Security Measures

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access and following 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://www.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	2026-07-10	Initial version