SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability Affecting Sentio Creator Extension 'Device Manager'

Document ID:	SCA-2026-0012
Publication Date:	2026-09-11
CVE Identifier:	CVE-2026-80469
CVSSv3 Base Score:	8.3
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
Version:	1

Summary

The Device Manager extension shipped with Sentio Creator is affected by CVE-2026-80469. Affected versions are pre-installed in Sentio Creator releases up to and including version 2026.2. As the Device Manager extension can be updated independently of Sentio Creator, SICK recommends applying the defined remediations for this vulnerability.

List of Products

Product	Affected by
Sentio Creator <=2026.2 using Device Manager <=1.4	CVE-2026-80469 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2026-80469 Improper Verification of Cryptographic Signature

Summary: An attacker may achieve arbitrary code execution on a target system by uploading a malicious device driver package, bypassing driver verification mechanisms, and triggering the execution of attacker-controlled code. User interaction is required.

CVE-2026-80469 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CWE identifier: CWE-347 (Improper Verification of Cryptographic Signature)

Remediations

Vendor Fix for CVE-2026-80469

Details: Users are strongly recommended to upgrade the Device Manager extension for Sentio Creator to version 1.4.1.

Valid for:

- Sentio Creator <=2026.2 using Device Manager <=1.4

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	2026-09-11	Initial version