

SICK PSIRT Security Advisory

Fast-xml-parser vulnerabilities affect Sentio Creator Extension 'Device Manager'

Document ID: sca-2026-0014

Publication Date: 2026-10-14

CVE Identifier: CVE-2026-27942, CVE-2026-25896, CVE-2026-26278

Version: 1

Summary

Multiple vulnerabilities in the third-party component fast-xml-parser affect the Device Manager Extension in Sentio Creator. The extension is maintained and updated independently from SICK Sentio Creator, but successful exploitation of these vulnerabilities could impact the security of the Sentio Creator. SICK strongly recommends upgrading the extension to remediate the identified issues.

List of Products

Product	Details
Sentio Creator all versions using Device Manager Version < 1.1.1	<u>Status:</u> Known Affected <u>Remediation:</u> Vendor Fix <u>CVE IDs:</u> CVE-2026-25896, CVE-2026-26278, CVE-2026-27942

Vulnerability Overview

CVE-2026-27942 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Summary: fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. Prior to version 5.3.8, the application crashes with stack overflow when user use XML builder with `preserveOrder:true`. Version 5.3.8 fixes the issue. As a workaround, use XML builder with `preserveOrder:false` or check the input data before passing to builder.

CVSSv3.1 base score: 5.3

CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CWE identifier: CWE-120 (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))

Remediations:

Product	Details
Sentio Creator all versions using Device Manager Version < 1.1.1	<u>Vendor Fix</u> It is strongly recommended to upgrade the Device Manger Extension to version 1.1.1.

CVE-2026-25896 Incorrect Regular Expression

Summary: fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. From 4.1.3 to before 5.3.5, a dot (.) in a DOCTYPE entity name is treated as a regex wildcard during entity replacement, allowing an attacker to shadow built-in XML entities (<, >, &, ", ') with arbitrary values. This bypasses entity encoding and leads to XSS when parsed output is rendered. This vulnerability is fixed in 5.3.5.

CVSSv3.1 base score: 9.3

CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N

CWE identifier: CWE-185 (Incorrect Regular Expression)

Remediations:

Product	Details
Sentio Creator all versions using Device Manager Version < 1.1.1	<u>Vendor Fix</u> It is strongly recommended to upgrade the Device Manger Extension to version 1.1.1.

CVE-2026-26278 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

Summary: fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. In versions 4.1.3 through 5.3.5, the XML parser can be forced to do an unlimited amount of entity expansion. With a very small XML input, it's possible to make the parser spend seconds or even minutes processing a single request, effectively freezing the application. Version 5.3.6 fixes the issue. As a workaround, avoid using DOCTYPE parsing by `processEntities: false` option.

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-776 (Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'))

Remediations:

Product	Details
Sentio Creator all versions using Device Manager Version < 1.1.1	<u>Vendor Fix</u> It is strongly recommended to upgrade the Device Manger Extension to version 1.1.1.

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>

The canonical URL.:

<https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0014.json>

History

Version	Release Date	Comment
1	2026-10-14	Initial version