SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities Affecting SICK CorivaEngine

Document ID:	sca-2026-0013
Publication Date:	2026-09-11
CVE Identifiers:	CVE-2026-59898, CVE-2026-59899, CVE-2026-47825
Version:	1

Summary

SICK CorivaEngine includes the third-party components Netty and Spring Cloud Gateway that are affected by multiple known vulnerabilities. Under certain conditions, these vulnerabilities could allow remote attackers to perform HTTP request smuggling, cause resource exhaustion, or manipulate forwarded request headers. Successful exploitation may impact the integrity and availability of affected systems. SICK has addressed these vulnerabilities and recommends that customers apply the remediations described in this Security Advisory.

List of Products

Product	Part Number	Affected by
SICK CorivaEngine <=2026.1.0	1619728	CVE-2026-59898 Status: Known Affected Remediation: Vendor fix
		CVE-2026-59899 Status: Known Affected Remediation: Vendor fix
		CVE-2026-47825 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2026-59898 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Summary: Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, ab attacker can force WebSocket upgrade via the lax V07 (or V08) handshaker by sending Sec–WebSocket–Version: 7 and omitting Connection: Upgrade / Upgrade: websocket headers, completing a protocol switch that a proxy would not recognize as an Upgrade request and enabling HTTP request smuggling / protocol-confusion attacks. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.

CVE-2026-59898 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:H/A:N
CWE identifier: CWE-444 (Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'))

CVE-2026-59899 Allocation of Resources Without Limits or Throttling

Summary: Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, HttpContentEncoder (the superclass of the production handler HttpContentCompressor) maintains a per-channel ArrayDeque<CharSequence> named acceptEncodingQueue that accumulates attacker-controlled data without any size limit. The queue is filled on the I/O thread for every inbound HTTP request and drained only when the application later writes a non-1xx response. This creates a resource exhaustion vulnerability when an attacker exploits HTTP/1.1 pipelining to flood the connection with requests faster than the application produces responses. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.

CVE-2026-59899 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-770 (Allocation of Resources Without Limits or Throttling)

CVE-2026-47825 Origin Validation Error

Summary: Spring Cloud Gateway Server forwards the X-Forwarded-For and Forwarded headers from untrusted proxies in certain configuration scenarios. This affects both the WebMVC and WebFlux Gateway Servers. Affected versions: Spring Cloud Gateway 3.1.x (fix 3.1.13). Spring Cloud Gateway 4.1.x (fix 4.1.13). Spring Cloud Gateway 4.2.x (fix 4.2.9). Spring Cloud Gateway 4.3.x (fix 4.3.5). Spring Cloud Gateway 5.0.x (fix 5.0.2).

CVE-2026-47825 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N
CWE identifier: CWE-346 (Origin Validation Error)

Remediations

Vendor Fix for CVE-2026-59898

Details: Users are recommended to upgrade to version 2026.1.1.

Valid for:

- SICK CorivaEngine <=2026.1.0

Vendor Fix for CVE-2026-59899

Details: Users are recommended to upgrade to version 2026.1.1.

Valid for:

- SICK CorivaEngine <=2026.1.0

Vendor Fix for CVE-2026-47825

Details: Users are recommended to upgrade to version 2026.1.1.

Valid for:

- SICK CorivaEngine <=2026.1.0

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	2026-09-11	Initial version