SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Multiple vulnerabilities in SICK Enterprise Analytics and SICK Logistic Analytics Products

Document ID:	SCA-2025-0010
Publication Date:	2026-05-13
CVE Identifiers:	CVE-2025-9914, CVE-2025-9913, CVE-2025-58587, CVE-2025-49184, CVE-2025-58589, CVE-2025-58590, CVE-2025-58591, CVE-2025-58584, CVE-2025-58585, CVE-2025-58586, CVE-2025-58579, CVE-2025-58583, CVE-2025-58581, CVE-2025-58580, CVE-2025-58582, CVE-2025-58578, CVE-2025-49186, CVE-2025-49193
Version:	2

Summary

SICK has found multiple vulnerabilities in SICK Enterprise Analytics and the SICK Logistic Analytics products. The vulnerabilities could potentially affect the confidentiality, integrity and availability of the products. Therefore it is strongly recommended to apply general security practices when operating the products. Currently, SICK is not aware of any public exploits.

List of Products

Product	Affected by
SICK Baggage Analytics <4.6.2	CVE-2025-58590 Status: Known Affected Remediation: Vendor fix
SICK Baggage Analytics <4.6.3	CVE-2025-9914 Status: Known Affected Remediation: Vendor fix
	CVE-2025-9913 Status: Known Affected Remediation: Vendor fix

	CVE-2025-58587 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58589 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58591 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58584 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58585 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58586 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58579 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49186 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49193 Status: Known Affected Remediation: Vendor fix
SICK Baggage Analytics all versions	CVE-2025-49184 Status: Known Affected Remediation: Workaround
SICK Enterprise Analytics all versions	CVE-2025-49184 Status: Known Affected Remediation: Workaround
	CVE-2025-58584 Status: Known Affected Remediation: Workaround

	CVE-2025-58586 Status: Known Affected Remediation: Workaround
	CVE-2025-58579 Status: Known Affected Remediation: Workaround
	CVE-2025-58583 Status: Known Affected Remediation: Workaround
	CVE-2025-58581 Status: Known Affected Remediation: Workaround
	CVE-2025-58580 Status: Known Affected Remediation: Workaround
	CVE-2025-58582 Status: Known Affected Remediation: Workaround
	CVE-2025-58578 Status: Known Affected Remediation: Workaround
SICK Logistic Diagnostic Analytics <4.6.2	CVE-2025-58590 Status: Known Affected Remediation: Vendor fix
SICK Logistic Diagnostic Analytics <4.6.3	CVE-2025-9914 Status: Known Affected Remediation: Vendor fix
	CVE-2025-9913 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58587 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58589 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58591 Status: Known Affected Remediation: Vendor fix

	CVE-2025-58584 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58585 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58586 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58579 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49186 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49193 Status: Known Affected Remediation: Vendor fix
SICK Logistic Diagnostic Analytics all versions	CVE-2025-49184 Status: Known Affected Remediation: Workaround
SICK Package Analytics <4.6.2	CVE-2025-58590 Status: Known Affected Remediation: Vendor fix
SICK Package Analytics <4.6.3	CVE-2025-9914 Status: Known Affected Remediation: Vendor fix
	CVE-2025-9913 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58587 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58589 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58591 Status: Known Affected Remediation: Vendor fix

	CVE-2025-58584 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58585 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58586 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58579 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49186 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49193 Status: Known Affected Remediation: Vendor fix
SICK Package Analytics all versions	CVE-2025-49184 Status: Known Affected Remediation: Workaround
SICK Tire Analytics <4.6.2	CVE-2025-58590 Status: Known Affected Remediation: Vendor fix
SICK Tire Analytics <4.6.3	CVE-2025-9914 Status: Known Affected Remediation: Vendor fix
	CVE-2025-9913 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58587 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58589 Status: Known Affected Remediation: Vendor fix

	CVE-2025-58591 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58584 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58585 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58586 Status: Known Affected Remediation: Vendor fix
	CVE-2025-58579 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49186 Status: Known Affected Remediation: Vendor fix
	CVE-2025-49193 Status: Known Affected Remediation: Vendor fix
SICK Tire Analytics all versions	CVE-2025-49184 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2025-9914 Authentication Bypass Using an Alternate Path or Channel

Summary: The credentials of the users stored in the system's local database can be used for the log in, making it possible for an attacker to gain unauthorized access. This could potentially affect the confidentiality of the application.

CVE-2025-9914 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-288 (Authentication Bypass Using an Alternate Path or Channel)

CVE-2025-9913 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: JavaScript can be run inside the address bar via the dashboard "Open in new Tab" button, making the application vulnerable to session hijacking.

CVE-2025-9913 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2025-58587 Improper Restriction of Excessive Authentication Attempts

Summary: The application does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it possible for an attacker to guess user credentials.

CVE-2025-58587 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
CWE identifier: CWE-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2025-49184 Exposure of Sensitive Information to an Unauthorized Actor

Summary: A remote unauthorized attacker may gather sensitive information of the application, due to missing authorization of configuration settings of the product.

CVE-2025-49184 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:H/I:N/A:N
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2025-58589 Exposure of Sensitive Information to an Unauthorized Actor

Summary: When an error occurs in the application a full stacktrace is provided to the user. The stacktrace lists class and method names as well as other internal information. An attacker thus receives information about the technology used and the structure of the application.

CVE-2025-58589 has been assigned to this vulnerability.
CVSSv3.1 base score: 2.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2025-58590 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Summary: It's possible to brute force folders and files, which can be used by an attacker to steal sensitive information.

CVE-2025-58590 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-22 (Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'))

CVE-2025-58591 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Summary: A remote, unauthorized attacker can brute force folders and files and read them like private keys or configurations, making the application vulnerable for gathering sensitive information.

CVE-2025-58591 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-22 (Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'))

CVE-2025-58584 Use of GET Request Method With Sensitive Query Strings

Summary: In the HTTP request, the username and password are transferred directly in the URL as parameters. However, URLs can be stored in various systems such as server logs, browser histories or proxy servers. As a result, there is a high risk that this sensitive data will be disclosed unintentionally.

CVE-2025-58584 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-598 (Use of GET Request Method With Sensitive Query Strings)

CVE-2025-58585 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Summary: Multiple endpoints with sensitive information do not require authentication, making the application susceptible to information gathering.

CVE-2025-58585 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-497 (Exposure of Sensitive System Information to an Unauthorized Control Sphere)

CVE-2025-58586 Observable Response Discrepancy

Summary: For failed login attempts, the application returns different error messages depending on whether the login failed due to an incorrect password or a non-existing username. This allows an attacker to guess usernames until they find an existing one.

CVE-2025-58586 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-204 (Observable Response Discrepancy)

CVE-2025-58579 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Summary: Due to a lack of authentication, it is possible for an unauthenticated user to request data from this endpoint, making the application vulnerable for user enumeration.

CVE-2025-58579 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-497 (Exposure of Sensitive System Information to an Unauthorized Control Sphere)

CVE-2025-58583 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Summary: The application provides access to a login protected H2 database for caching purposes. The username is prefilled.

CVE-2025-58583 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-497 (Exposure of Sensitive System Information to an Unauthorized Control Sphere)

CVE-2025-58581 Exposure of Sensitive Information to an Unauthorized Actor

Summary: When an error occurs in the application a full stacktrace is provided to the user. The stacktrace lists class and method names as well as other internal information. An attacker can thus obtain information about the technology used and the structure of the application.

CVE-2025-58581 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2025-58580 Improper Output Neutralization for Logs

Summary: An API endpoint allows arbitrary log entries to be created via POST request. Without sufficient validation of the input data, an attacker can create manipulated log entries and thus falsify or dilute logs, for example.

CVE-2025-58580 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
CWE identifier: CWE-117 (Improper Output Neutralization for Logs)

CVE-2025-58582 Allocation of Resources Without Limits or Throttling

Summary: If a user tries to login but the provided credentials are incorrect a log is created. The data for this POST requests is not validated and it's possible to send giant payloads which are then logged.

CVE-2025-58582 has been assigned to this vulnerability.
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-770 (Allocation of Resources Without Limits or Throttling)

CVE-2025-58578 Allocation of Resources Without Limits or Throttling

Summary: A user with the appropriate authorization can create any number of user accounts via an API endpoint using a POST request. There are no quotas, checking mechanisms or restrictions to limit the creation.

CVE-2025-58578 has been assigned to this vulnerability.
CVSSv3.1 base score: 3.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

CVE-2025-49186 Improper Restriction of Excessive Authentication Attempts

Summary: The product does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it susceptible to brute-force attacks.

CVE-2025-49186 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2025-49193 Protection Mechanism Failure

Summary: The application fails to implement several security headers. These headers help increase the overall security level of the web application by e.g., preventing the application to be displayed in an iFrame (Clickjacking attacks) or not executing injected malicious JavaScript code (XSS attacks).

CVE-2025-49193 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
CWE identifier: CWE-693 (Protection Mechanism Failure)

Remediations

Vendor Fix for CVE-2025-9914

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-9913

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-58587

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Workaround for CVE-2025-58587

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-49184

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Baggage Analytics all versions
- SICK Enterprise Analytics all versions
- SICK Logistic Diagnostic Analytics all versions
- SICK Package Analytics all versions
- SICK Tire Analytics all versions

Vendor Fix for CVE-2025-58589

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-58590

Details: It is strongly recommended to update to the latest version (>= 4.6.2).

Valid for:

- SICK Baggage Analytics <4.6.2
- SICK Logistic Diagnostic Analytics <4.6.2
- SICK Package Analytics <4.6.2
- SICK Tire Analytics <4.6.2

Vendor Fix for CVE-2025-58591

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-58584

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Workaround for CVE-2025-58584

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Vendor Fix for CVE-2025-58585

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-58586

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Workaround for CVE-2025-58586

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Vendor Fix for CVE-2025-58579

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Workaround for CVE-2025-58579

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-58583

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-58581

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-58580

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-58582

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Workaround for CVE-2025-58578

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK Enterprise Analytics all versions

Vendor Fix for CVE-2025-49186

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

Vendor Fix for CVE-2025-49193

Details: It is strongly recommended to update the product to version 4.6.3.

Valid for:

- SICK Baggage Analytics <4.6.3
- SICK Logistic Diagnostic Analytics <4.6.3
- SICK Package Analytics <4.6.3
- SICK Tire Analytics <4.6.3

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://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	2025-10-02	Initial version
2	2026-05-13	Fixes for the products Baggage Analytics, Package Analytics, Tire Analytics, Logistic Diagnostic Analytics.