TLP:WHITE

SICK PSIRT
Security Advisory

Multiple vulnerabilities in SICK Field Analytics and SICK Media Server

Document ID:	SCA-2025-0007
Publication Date:	2025-06-12
CVE Identifiers:	CVE-2025-49181, CVE-2025-49182, CVE-2025-49183, CVE-2025-49184, CVE-2025-49185, CVE-2025-49186, CVE-2025-49187, CVE-2025-49188, CVE-2025-49189, CVE-2025-49190, CVE-2025-49191, CVE-2025-49192, CVE-2025-49193, CVE-2025-49194, CVE-2025-49195, CVE-2025-49196, CVE-2025-49197, CVE-2025-49198, CVE-2025-49199, CVE-2025-49200
Version:	2

Summary

SICK has found multiple vulnerabilities in the products SICK Field Analytics and SICK Media Server. The vulnerabilities could potentially affect the confidentiality, integrity an 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	Part Number	Affected by
SICK Field Analytics all versions	1613101	CVE-2025-49184 Status: Known Affected Remediation: Workaround
		CVE-2025-49185 Status: Known Affected Remediation: Workaround
		CVE-2025-49186 Status: Known Affected Remediation: Workaround

		CVE-2025-49187 Status: Known Affected Remediation: Workaround
		CVE-2025-49188 Status: Known Affected Remediation: Workaround
		CVE-2025-49190 Status: Known Affected Remediation: Workaround
		CVE-2025-49191 Status: Known Affected Remediation: Workaround
		CVE-2025-49192 Status: Known Affected Remediation: Workaround
		CVE-2025-49193 Status: Known Affected Remediation: Workaround
		CVE-2025-49196 Status: Known Affected Remediation: Workaround
		CVE-2025-49199 Status: Known Affected Remediation: Workaround
		CVE-2025-49200 Status: Known Affected Remediation: Workaround
SICK Media Server <= 1.4		CVE-2025-49182 Status: Known Affected Remediation: Vendor fix
		CVE-2025-49189 Status: Known Affected Remediation: Vendor fix
		CVE-2025-49192 Status: Known Affected Remediation: Vendor fix
		CVE-2025-49193 Status: Known Affected Remediation: Vendor fix

		CVE-2025-49197 Status: Known Affected Remediation: Vendor fix
SICK Media Server all versions		CVE-2025-49181 Status: Known Affected Remediation: Mitigation
		CVE-2025-49183 Status: Known Affected Remediation: Workaround
		CVE-2025-49186 Status: Known Affected Remediation: Workaround
		CVE-2025-49194 Status: Known Affected Remediation: Workaround
		CVE-2025-49195 Status: Known Affected Remediation: Workaround
		CVE-2025-49198 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2025-49181 Missing Authorization

Summary: Due to missing authorization of an API endpoint, unauthorized users can send HTTP GET requests to gather sensitive information. An attacker could also send HTTP POST requests to modify the log files' root path as well as the TCP ports the service is running on, leading to a Denial of Service attack.

CVE-2025-49181 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:U/C:L/I:L/A:H
CWE identifier: CWE-862 (Missing Authorization)

CVE-2025-49182 Inclusion of Sensitive Information in Source Code

Summary: Files in the source code contain login credentials for the admin user and the property configuration password, allowing an attacker to get full access to the application.

CVE-2025-49182 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-540 (Inclusion of Sensitive Information in Source Code)

CVE-2025-49183 Cleartext Transmission of Sensitive Information

Summary: All communication with the REST API is unencrypted (HTTP), allowing an attacker to intercept traffic between an actor and the webserver. This leads to the possibility of information gathering and downloading media files.

CVE-2025-49183 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-319 (Cleartext Transmission of Sensitive Information)

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-2025-49185 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: The web application is susceptible to cross-site-scripting attacks. An attacker who can create new dashboard widgets can inject malicious JavaScript code into the Transform Function which will be executed when the widget receives data from its data source.

CVE-2025-49185 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

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-2025-49187 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-2025-49187 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-2025-49188 Use of GET Request Method With Sensitive Query Strings

Summary: The application sends user credentials as URL parameters instead of POST bodies, making it vulnerable to information gathering.

CVE-2025-49188 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-2025-49189 Sensitive Cookie Without 'HttpOnly' Flag

Summary: The HttpOnlyflag of the session cookie "@@" is set to false. Since this flag helps preventing access to cookies via client-side scripts, setting the flag to false can lead to a higher possibility of Cross-Side-Scripting attacks which target the stored cookies.

CVE-2025-49189 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-1004 (Sensitive Cookie Without 'HttpOnly' Flag)

CVE-2025-49190 Server-Side Request Forgery (SSRF)

Summary: The application is vulnerable to Server-Side Request Forgery (SSRF). An endpoint can be used to send server internal requests to other ports.

CVE-2025-49190 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-918 (Server-Side Request Forgery (SSRF))

CVE-2025-49191 Improper Restriction of Rendered UI Layers or Frames

Summary: Linked URLs during the creation of iFrame widgets and dashboards are vulnerable to code execution. The URLs get embedded as iFrame widgets, making it possible to attack other users that access the dashboard by including malicious code. The attack is only possible if the attacker is authorized to create new dashboards or iFrame widgets.

CVE-2025-49191 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
CWE identifier: CWE-1021 (Improper Restriction of Rendered UI Layers or Frames)

CVE-2025-49192 Improper Restriction of Rendered UI Layers or Frames

Summary: The web application is vulnerable to clickjacking attacks. The site can be embedded into another frame, allowing an attacker to trick a user into clicking on something different from what the user perceives. This could potentially reveal confidential information or allow others to take control of their computer while clicking on seemingly innocuous objects.

CVE-2025-49192 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE identifier: CWE-1021 (Improper Restriction of Rendered UI Layers or Frames)

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)

CVE-2025-49194 Cleartext Transmission of Sensitive Information

Summary: The server supports authentication methods in which credentials are sent in plaintext over unencrypted channels. If an attacker were to intercept traffic between a client and this server, the credentials would be exposed.

CVE-2025-49194 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-319 (Cleartext Transmission of Sensitive Information)

CVE-2025-49195 Improper Restriction of Excessive Authentication Attempts

Summary: The FTP server's login mechanism does not restrict authentication attempts, allowing an attacker to brute-force user passwords and potentially compromising the FTP server.

CVE-2025-49195 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-2025-49196 Use of a Broken or Risky Cryptographic Algorithm

Summary: A service supports the use of a deprecated and unsafe TLS version. This could be exploited to expose sensitive information, modify data in unexpected ways or spoof identities of other users or devices, affecting the confidentiality and integrity of the device.

CVE-2025-49196 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2025-49197 Use of Weak Hash

Summary: The application uses a weak password hash function, allowing an attacker to crack the weak password hash to gain access to an FTP user account.

CVE-2025-49197 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-328 (Use of Weak Hash)

CVE-2025-49198 Use of Insufficiently Random Values

Summary: The Media Server's authorization tokens have a poor quality of randomness. An attacker may be able to guess the token of an active user by computing plausible tokens.

CVE-2025-49198 has been assigned to this vulnerability.
CVSSv3.1 base score: 3.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CWE identifier: CWE-330 (Use of Insufficiently Random Values)

CVE-2025-49199 Insufficient Verification of Data Authenticity

Summary: The backup ZIPs are not signed by the application, leading to the possibility that an attacker can download a backup ZIP, modify and re-upload it. This allows the attacker to disrupt the application by configuring the services in a way that they are unable to run, making the application unusable. They can redirect traffic that is meant to be internal to their own hosted services and gathering information.

CVE-2025-49199 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-345 (Insufficient Verification of Data Authenticity)

CVE-2025-49200 Exposure of Sensitive Information to an Unauthorized Actor

Summary: The created backup files are unencrypted, making the application vulnerable for gathering sensitive information by downloading and decompressing the backup files.

CVE-2025-49200 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-200 (Exposure of Sensitive Information to an Unauthorized Actor)

Remediations

Mitigation for CVE-2025-49181

Details: It is possible to enable the authorization of the API endpoint via licence. Please contact your support to get a licence with API authorization enabled.

Valid for:

- SICK Media Server all versions

Vendor Fix for CVE-2025-49182

Details: Users are strongly recommended to upgrade to the latest release of Media Server (>= 1.5). It is also advised to change the default passwords.

Valid for:

- SICK Media Server <= 1.4

Workaround for CVE-2025-49183

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 Media Server 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 Field Analytics all versions

Workaround for CVE-2025-49185

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 Field Analytics all versions

Workaround for CVE-2025-49186

Details: It is highly recommended to use a strong password with a length of at least eight characters and a combination of letters, numbers, capital letters and symbols. Please make also 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 Field Analytics all versions
- SICK Media Server all versions

Workaround for CVE-2025-49187

Details: It is highly recommended to use a strong password with a length of at least eight characters and a combination of letters, numbers, capital letters and symbols. 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 Field Analytics all versions

Workaround for CVE-2025-49188

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 Field Analytics all versions

Vendor Fix for CVE-2025-49189

Details: Users are strongly recommended to upgrade to the latest release of Media Server (>= 1.5).

Valid for:

- SICK Media Server <= 1.4

Workaround for CVE-2025-49190

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 Field Analytics all versions

Workaround for CVE-2025-49191

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 Field Analytics all versions

Vendor Fix for CVE-2025-49192

Details: Users are strongly recommended to upgrade to the latest release of Media Server (>= 1.5).

Valid for:

- SICK Media Server <= 1.4

Workaround for CVE-2025-49192

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 Field Analytics all versions

Vendor Fix for CVE-2025-49193

Details: Users are strongly recommended to upgrade to the latest release of Media Server (>= 1.5).

Valid for:

- SICK Media Server <= 1.4

Workaround for CVE-2025-49193

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 Field Analytics all versions

Workaround for CVE-2025-49194

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 Media Server all versions

Workaround for CVE-2025-49195

Details: It is highly recommended to use a strong password with a length of at least eight characters and a combination of letters, numbers, capital letters and symbols. 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 Media Server all versions

Workaround for CVE-2025-49196

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 Field Analytics all versions

Vendor Fix for CVE-2025-49197

Details: It is strongly recommended to upgrade to the latest version.

Valid for:

- SICK Media Server <= 1.4

Workaround for CVE-2025-49198

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 Media Server all versions

Workaround for CVE-2025-49199

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 Field Analytics all versions

Workaround for CVE-2025-49200

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 Field Analytics all versions

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	2025-06-12	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated