TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities affecting SICK TDC-X401GL

Document ID:	SCA-2026-0001
Publication Date:	2026-01-15
CVE Identifiers:	CVE-2026-22907, CVE-2024-10771, CVE-2026-22908, CVE-2026-22909, CVE-2026-22910, CVE-2026-22911, CVE-2026-22912, CVE-2026-22913, CVE-2026-22914, CVE-2026-22915, CVE-2026-22916, CVE-2026-22917, CVE-2026-22918, CVE-2026-22919, CVE-2025-32471
Version:	2

Summary

SICK has identified multiple vulnerabilities in the SICK TDC-X401GL product. The vulnerabilities could potentially affect the confidentiality, integrity an availability of the product. Therefore it is strongly recommended to apply general security practices when operating the product. SICK is currently not aware of any public exploits.

List of Products

Product	Part Number	Affected by
SICK TDC-X401GL all Firmware versions	1139622	CVE-2024-10771 Status: Known Affected Remediation: Workaround
		CVE-2026-22909 Status: Known Affected Remediation: Workaround
		CVE-2026-22910 Status: Known Affected Remediation: Workaround

		CVE-2026-22911 Status: Known Affected Remediation: Mitigation
		CVE-2026-22914 Status: Known Affected Remediation: Workaround
		CVE-2026-22915 Status: Known Affected Remediation: Workaround
		CVE-2026-22916 Status: Known Affected Remediation: Workaround
		CVE-2026-22918 Status: Known Affected Remediation: Mitigation
		CVE-2025-32471 Status: Known Affected Remediation: Workaround
SICK TDC-X401GL with Firmware <1.4.0	1139622	CVE-2026-22907 Status: Known Affected Remediation: Vendor fix
		CVE-2026-22908 Status: Known Affected Remediation: Vendor fix
SICK TDC-X401GL with Firmware <1.5.0	1139622	CVE-2026-22912 Status: Known Affected Remediation: Vendor fix
		CVE-2026-22913 Status: Known Affected Remediation: Vendor fix
		CVE-2026-22917 Status: Known Affected Remediation: Vendor fix
		CVE-2026-22919 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2026-22907 Incorrect Privilege Assignment

Summary: An attacker may gain unauthorized access to the host filesystem, potentially allowing them to read and modify system data.

CVE-2026-22907 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-266 (Incorrect Privilege Assignment)

CVE-2024-10771 Improper Control of Generation of Code ('Code Injection')

Summary: Due to missing input validation during one step of the firmware update process, the product is vulnerable to remote code execution. With network access and the user level "Service", an attacker can execute arbitrary system commands in the root user's contexts.

CVE-2024-10771 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-94 (Improper Control of Generation of Code ('Code Injection'))

CVE-2026-22908 Incorrect Privilege Assignment

Summary: Uploading unvalidated container images may allow remote attackers to gain full access to the system, potentially compromising its integrity and confidentiality.

CVE-2026-22908 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-266 (Incorrect Privilege Assignment)

CVE-2026-22909 Improper Access Control

Summary: Certain system functions may be accessed without proper authorization, allowing attackers to start, stop, or delete installed applications, potentially disrupting system operations.

CVE-2026-22909 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-284 (Improper Access Control)

CVE-2026-22910 Use of Weak Credentials

Summary: The device is deployed with weak and publicly known default passwords for certain hidden user levels, increasing the risk of unauthorized access. This represents a high risk to the integrity of the system.

CVE-2026-22910 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-1391 (Use of Weak Credentials)

CVE-2026-22911 Use of Hard-coded Credentials

Summary: Firmware update files may expose password hashes for system accounts, which could allow a remote attacker to recover credentials and gain unauthorized access to the device.

CVE-2026-22911 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-798 (Use of Hard-coded Credentials)

CVE-2026-22912 URL Redirection to Untrusted Site ('Open Redirect')

Summary: Improper validation of a login parameter may allow attackers to redirect users to malicious websites after authentication. This can lead to various risk including stealing credentials from unsuspecting users.

CVE-2026-22912 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:L/I:N/A:N
CWE identifier: CWE-601 (URL Redirection to Untrusted Site ('Open Redirect'))

CVE-2026-22913 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: Improper handling of a URL parameter may allow attackers to execute code in a user's browser after login. This can lead to the extraction of sensitive data.

CVE-2026-22913 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:L/I:N/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2026-22914 Incorrect Privilege Assignment

Summary: An attacker with limited permissions may still be able to write files to specific locations on the device, potentially leading to system manipulation.

CVE-2026-22914 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:N/I:L/A:N
CWE identifier: CWE-266 (Incorrect Privilege Assignment)

CVE-2026-22915 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Summary: An attacker with low privileges may be able to read files from specific directories on the device, potentially exposing sensitive information.

CVE-2026-22915 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-497 (Exposure of Sensitive System Information to an Unauthorized Control Sphere)

CVE-2026-22916 Incorrect Privilege Assignment

Summary: An attacker with low privileges may be able to trigger critical system functions such as reboot or factory reset without proper restrictions, potentially leading to service disruption or loss of configuration.

CVE-2026-22916 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:N/I:N/A:L
CWE identifier: CWE-266 (Incorrect Privilege Assignment)

CVE-2026-22917 Allocation of Resources Without Limits or Throttling

Summary: Improper input handling in a system endpoint may allow attackers to overload resources, causing a denial of service.

CVE-2026-22917 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:N/I:N/A:L
CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

CVE-2026-22918 Improper Restriction of Rendered UI Layers or Frames

Summary: An attacker may exploit missing protection against clickjacking by tricking users into performing unintended actions through maliciously crafted web pages, leading to the extraction of sensitive data.

CVE-2026-22918 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-2026-22919 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: An attacker with administrative access may inject malicious content into the login page, potentially enabling cross-site scripting (XSS) attacks, leading to the extraction of sensitive data.

CVE-2026-22919 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:L/I:L/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2025-32471 Use of Weak Credentials

Summary: The device's passwords have not been adequately salted, making them vulnerable to password extraction attacks.

CVE-2025-32471 has been assigned to this vulnerability.
CVSSv3.1 base score: 3.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-1391 (Use of Weak Credentials)

Remediations

Vendor Fix for CVE-2026-22907

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.4.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.4.0

Workaround for CVE-2024-10771

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Vendor Fix for CVE-2026-22908

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.4.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.4.0

Workaround for CVE-2026-22909

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Workaround for CVE-2026-22910

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Mitigation for CVE-2026-22911

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 TDC-X401GL all Firmware versions

Vendor Fix for CVE-2026-22912

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.5.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.5.0

Vendor Fix for CVE-2026-22913

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.5.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.5.0

Workaround for CVE-2026-22914

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Workaround for CVE-2026-22915

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Workaround for CVE-2026-22916

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware versions

Vendor Fix for CVE-2026-22917

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.5.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.5.0

Mitigation for CVE-2026-22918

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 TDC-X401GL all Firmware versions

Vendor Fix for CVE-2026-22919

Details: Users are strongly recommended to upgrade to the latest release of TDC-X401GL (>= 1.5.0).

Valid for:

- SICK TDC-X401GL with Firmware <1.5.0

Workaround for CVE-2025-32471

Details: Upon completion of the initial device setup, deactivate AppEngine. Disabling it fully mitigates this vulnerability.

Valid for:

- SICK TDC-X401GL all Firmware 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	2026-01-15	Initial version
2	2026-05-12	Updated CVE Record