

SICK PSIRT Security Advisory

Vulnerabilities affecting SICK Incoming Goods Suite

Document ID: SCA-2026-0002
Publication Date: 2026-01-22
CVE Identifiers: CVE-2025-6023, CVE-2025-3260, CVE-2025-2703, CVE-2025-4123, CVE-2025-3415, CVE-2025-3580, CVE-2025-3454, CVE-2025-6197, CVE-2025-1088, CVE-2026-22644, CVE-2026-22645, CVE-2026-22646
Version: 2

Summary

SICK has identified multiple vulnerabilities in the SICK Incoming Goods Suite product. Vulnerabilities related to Grafana apply exclusively to the administrative user interface for log management and do not affect the Incoming Goods Suite user interface. The vulnerabilities could potentially affect the confidentiality, integrity and availability of the product. Therefore it is strongly recommended to apply general security practices when operating the product.

List of Products

Product	Part Number	Affected by
SICK Incoming Goods Suite all Firmware versions	1139622	CVE-2026-22644 Status: Known Affected Remediation: Mitigation
SICK Incoming Goods Suite with Firmware <1.2.1	1139622	CVE-2025-6023 Status: Known Affected Remediation: Vendor fix
		CVE-2025-3260 Status: Known Affected Remediation: Vendor fix

	CVE-2025-2703 Status: Known Affected Remediation: Vendor fix
	CVE-2025-4123 Status: Known Affected Remediation: Vendor fix
	CVE-2025-3415 Status: Known Affected Remediation: Vendor fix
	CVE-2025-3580 Status: Known Affected Remediation: Vendor fix
	CVE-2025-3454 Status: Known Affected Remediation: Vendor fix
	CVE-2025-6197 Status: Known Affected Remediation: Vendor fix
	CVE-2025-1088 Status: Known Affected Remediation: Vendor fix
	CVE-2026-22645 Status: Known Affected Remediation: Vendor fix
	CVE-2026-22646 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

[CVE-2025-6023 URL Redirection to Untrusted Site \('Open Redirect'\)](#)

Summary: An open redirect vulnerability has been identified in Grafana OSS that can be exploited to achieve XSS attacks. The vulnerability was introduced in Grafana v11.5.0. The open redirect can be chained with path traversal vulnerabilities to achieve XSS. Fixed in versions 12.0.2+security-01, 11.6.3+security-01, 11.5.6+security-01, 11.4.6+security-01 and 11.3.8+security-01

CVE-2025-6023 has been assigned to this vulnerability.

CVSSv3.1 base score: 7.6

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

CWE identifier: CWE-601 (URL Redirection to Untrusted Site ('Open Redirect'))

CVE-2025-3260 Incorrect Authorization

Summary: A security vulnerability in the /apis/dashboard.grafana.app/* endpoints allows authenticated users to bypass dashboard and folder permissions. The vulnerability affects all API versions (v0alpha1, v1alpha1, v2alpha1). Impact: - Viewers can view all dashboards/folders regardless of permissions - Editors can view/edit/delete all dashboards/folders regardless of permissions - Editors can create dashboards in any folder regardless of permissions - Anonymous users with viewer/editor roles are similarly affected Organization isolation boundaries remain intact. The vulnerability only affects dashboard access and does not grant access to datasources.

CVE-2025-3260 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.3

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

CWE identifier: CWE-863 (Incorrect Authorization)

CVE-2025-2703 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: The built-in XY Chart plugin is vulnerable to a DOM XSS vulnerability. A user with Editor permissions is able to modify such a panel in order to make it execute arbitrary JavaScript.

CVE-2025-2703 has been assigned to this vulnerability.

CVSSv3.1 base score: 6.8

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

CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2025-4123 URL Redirection to Untrusted Site ('Open Redirect')

Summary: A cross-site scripting (XSS) vulnerability exists in Grafana caused by combining a client path traversal and open redirect. This allows attackers to redirect users to a website that hosts a frontend plugin that will execute arbitrary JavaScript. This vulnerability does not require editor permissions and if anonymous access is enabled, the XSS will work. If the Grafana Image Renderer plugin is installed, it is possible to exploit the open redirect to achieve a full read SSRF. The default Content-Security-Policy (CSP) in Grafana will block the XSS though the connect-src directive.

CVE-2025-4123 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.3

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

CWE identifier: CWE-601 (URL Redirection to Untrusted Site ('Open Redirect'))

CVE-2025-3415 Exposure of Sensitive Information to an Unauthorized Actor

Summary: Grafana is an open-source platform for monitoring and observability. The Grafana Alerting DingDing integration was not properly protected and could be exposed to users with Viewer permission. Fixed in versions 10.4.19+security-01, 11.2.10+security-01, 11.3.7+security-01, 11.4.5+security-01, 11.5.5+security-01, 11.6.2+security-01 and 12.0.1+security-01

CVE-2025-3415 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-2025-3580 Improper Access Control

Summary: An access control vulnerability was discovered in Grafana OSS where an Organization administrator could permanently delete the Server administrator account. This vulnerability exists in the DELETE /api/org/users/ endpoint. The vulnerability can be exploited when: 1. An Organization administrator exists 2. The Server administrator is either: - Not part of any organization, or - Part of the same organization as the Organization administrator Impact: - Organization administrators can permanently delete Server administrator accounts - If the only Server administrator is deleted, the Grafana instance becomes unmanageable - No super-user permissions remain in the system - Affects all users, organizations, and teams managed in the instance The vulnerability is particularly serious as it can lead to a complete loss of administrative control over the Grafana instance.

CVE-2025-3580 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:U/C:N/I:L/A:H

CWE identifier: CWE-284 (Improper Access Control)

CVE-2025-3454 Improper Authorization

Summary: This vulnerability in Grafana's datasource proxy API allows authorization checks to be bypassed by adding an extra slash character in the URL path. Users with minimal permissions could gain unauthorized read access to GET endpoints in Alertmanager and Prometheus datasources. The issue primarily affects datasources that implement route-specific permissions, including Alertmanager and certain Prometheus-based datasources.

CVE-2025-3454 has been assigned to this vulnerability.

CVSSv3.1 base score: 5

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

CWE identifier: CWE-285 (Improper Authorization)

CVE-2025-6197 URL Redirection to Untrusted Site ('Open Redirect')

Summary: An open redirect vulnerability has been identified in Grafana OSS organization switching functionality. Prerequisites for exploitation: - Multiple organizations must exist in the Grafana instance - Victim must be on a different organization than the one specified in the URL

CVE-2025-6197 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-601 (URL Redirection to Untrusted Site ('Open Redirect'))

CVE-2025-1088 Improper Input Validation

Summary: In Grafana, an excessively long dashboard title or panel name will cause Chromium browsers to become unresponsive due to Improper Input Validation vulnerability in Grafana. This issue affects Grafana: before 11.6.2 and is fixed in 11.6.2 and higher.

CVE-2025-1088 has been assigned to this vulnerability.

CVSSv3.1 base score: 8.3

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

CWE identifier: CWE-20 (Improper Input Validation)

CVE-2026-22644 Use of GET Request Method With Sensitive Query Strings

Summary: Certain requests pass the authentication token in the URL as string query parameter, making it vulnerable to theft through server logs, proxy logs and Referer headers, which could allow an attacker to hijack the user's session and gain unauthorized access.

CVE-2026-22644 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-2026-22645 Exposure of Sensitive Information to an Unauthorized Actor

Summary: The application discloses all used components, versions and license information to unauthenticated actors, giving attackers the opportunity to target known security vulnerabilities of used components.

CVE-2026-22645 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-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2026-22646 Generation of Error Message Containing Sensitive Information

Summary: Certain error messages returned by the application expose internal system details that should not be visible to end users, providing attackers with valuable reconnaissance information (like file paths, database errors, or software versions) that can be used to map the application's internal structure and discover other, more critical vulnerabilities.

CVE-2026-22646 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-209 (Generation of Error Message Containing Sensitive Information)

Remediations

Vendor Fix for CVE-2025-6023

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-3260

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-2703

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-4123

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-3415

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-3580

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-3454

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-6197

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2025-1088

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Mitigation for CVE-2026-22644

Details: Please make sure that logs exclude informative level and are stored in a secure way. For more information please follow the official Microsoft Security Considerations document for .NET: <https://learn.microsoft.com/en-us/aspnet/core/signalr/security?view=aspnetcore-9.0#access-token-logging> 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 Incoming Goods Suite all Firmware versions

Vendor Fix for CVE-2026-22645

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

Vendor Fix for CVE-2026-22646

Details: Users are strongly recommended to upgrade to the latest release of Incoming Goods Suite ($\geq 1.2.1$).

Valid for:

- SICK Incoming Goods Suite with Firmware $< 1.2.1$

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.



Sensor Intelligence.

TLP:WHITE

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	2026-01-22	Corrected CVE IDs

TLP:WHITE