swisslog healthcare | translogic a swisslog healthcare company

11080 Circle Point Road, Suite 500
Westminster, CO 80020

800.764.0300
swisslog-healthcare.com
translogic.com

CVE Date: November 3, 2026

Subject: CVE-2026-109618 / CVE-2026-109619

Vulnerability Name: PHP Vulnerabilities

Vulnerability Type: Unauthenticated remote code execution

Information: swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures

Summary

Swisslog Healthcare has identified a vulnerability in the pneumatic tube system product. If exploited, it could allow an unauthenticated user to execute remote code. A fix is available in tube system software versions 9.0.7 and 7.4.14. Swisslog Healthcare recommends that customers upgrade to one of these versions if they are currently on tube system software versions 7.4.9 and newer.

Affected Products

The following table lists the product impacted by the vulnerabilities listed above and the current state of remediation planning.

Product	Affected versions	Fixed version
ITS TU/Blower Boards	Series 1	Firmware v2.0.2 & v2.1.12
Pneumatic Tube System Software	v7.4.9 and newer	Software v7.4.14 & v9.0.7

Workaround and Mitigation

Swisslog Healthcare took the following actions:

- Upgraded to a patched PHP version 8.2.35 and developed a corresponding firmware release, along with hotfixes for software versions 9.0.7 and 7.4.14.
- While the exposure window is limited, it is strongly recommended that affected customers apply the software update once it becomes available to fully mitigate the vulnerability.

General Security Recommendations

- Follow established cybersecurity and access-control practices.
- Limit administrative access to authorized personnel only.

- Continue normal security monitoring procedures.

Vulnerability Classification

The vulnerability classification has been performed by using the CVSS scoring system in version 4.0. The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerabilities CVE-2026-109618 / CVE-2026-109619

Base Score: 9.2 (Critical) under CVSS v4.0 (specific to the customer's environment)

Impact Vector: Unauthenticated Network RCE. An attacker requires no privileges or user interaction to exploit them over HTTP/HTTPS.

See Scoring Reference: NVD CVSS v4.0 Calculator

Recommended Actions

Upgrade to version 7.4.14 or 9.0.7

Support and Contact Information

Customers with questions should contact the Customer Care Center at servicerequest.na@swisslog-healthcare.com / 1-800-396-9666.

To report a security vulnerability, contact slhcsecurity@swisslog-healthcare.com.

Disclaimer

This advisory is provided for informational purposes to help customers protect their systems. The information is based on what Swisslog Healthcare knows as of the date of publication and may be updated.