Statement:
TransLogic® Firmware Vulnerabilities

July 30, 2021

Swisslog Healthcare offers the following statement regarding potential security vulnerabilities that may exist in TransLogic® firmware driving a specific panel in some pneumatic tube systems. The vulnerabilities are limited to the HMI-3 circuit board inside of Nexus™ Panels when connected using an ethernet connection. These pneumatic tube systems are deployed primarily in hospitals within North America.

The potential vulnerabilities were identified as part of an assessment by Armis, an internationally recognized information security company, and investigated both in the current and prior releases of TransLogic firmware.

Jennie McQuade, Chief Privacy Officer for Swisslog Healthcare, notes that vulnerabilities only exist when a combination of variables exists. The potential for pneumatic tube stations (where the firmware is deployed) to be compromised is dependent on a bad actor who has access to the facility's information technology network and who could cause additional damage by leveraging these exploits.

The Software Engineering and Product Security Teams at Swisslog Healthcare have researched, reviewed, and confirmed potential vulnerabilities which could impact healthcare facilities currently using hardware containing the HMI3 panel when connected via Ethernet. A total of eight vulnerabilities have been found. Seven of these were subsequently removed in a software release containing updated firmware. Mitigations for the remaining vulnerability were made. Details on mitigations are documented in the company's Network Communications and Deployment Guide which is readily available to customers.

Steps Taken

Partnering closely with Armis, the following steps were taken following identification of the vulnerabilities:

1. Confirmed the identity of potentially affected files and versions.
2. Evaluated the firmware to assess the vulnerabilities and potential implications those vulnerabilities represent.
3. Provided Armis with versions of the current firmware and the subsequent release (not yet publicly available) to evaluate for the existence of vulnerabilities.

4. Established a lab environment to recreate the vulnerability.
5. Replicated vulnerabilities in the test lab environment.
6. Developed solutions to address the identified vulnerabilities.
7. Initiated customer contact to offer mitigation strategies and support for onsite IT security teams.

Because Swisslog Healthcare holds security as an organizational priority, our actionable security measures have prepared us to address these types of issues. Significant hardware and software programmatic actions include:

- Continuous analysis of software code
- Ongoing patching and testing of operating system compatibility
- Regular evaluation product line enhancements
- Continual collaboration with reputable third-party researchers
- Regular external audits of product, service, and security practices

Moving Forward

The privacy and the security of customer data are our highest priorities. Swisslog Healthcare is committed to continually monitoring our security programs and industry trends to offer proactive protection to our customers.

We are grateful to be a trusted provider of healthcare institutions around the world.

Next Steps for Swisslog Healthcare Customers

Please inquire with the Swisslog Healthcare Customer Care Team to determine the applicability of this notice to the pneumatic tube system installed in your facility(ies).

Direct any questions regarding these vulnerabilities and the mitigations to the Customer Care Team. Customer Care is available to current customers 24 hours, 7 days a week by calling 1-800-396-9666. Customers not currently under contract are asked to leave a voicemail, and those calls will be returned in the order they are received.

Thank you for your understanding.