Swisslog Healthcare
11325 Main Street
Broomfield, CO 80020

800.764.0300
healthcare.us@swisslog-healthcare.com
swisslog-healthcare.com

Date: August 2, 2021

Subject: CVE-2021-37165

Vulnerability Name: Overflow in hmiProcessMsg

Vulnerability Type: Buffer overflow

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

Summary

A buffer overflow issue was discovered in HMI-3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When a message is sent to the HMI TCP socket, it is forwarded to the hmiProcessMsg function through the pendingQ, and may lead to remote code execution.

Affected Products

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

Product	Fix Version	Target Release Date
HMI-3 Panel	7.2.5.7	August 2, 2021

Workaround and Mitigation

Network firewalls

Network firewalls that restrict inter-VLAN traffic on the network must allow inbound and outbound internal network connections for the ports listed in “Windows firewalls”. Do not restrict these ports to specific applications.

Layer 3 Access Control List

If there is no firewall between the SCC and the floor devices, apply an extended access control list (ACL) in the layer 3 VLAN that is dedicated to the PTS floor equipment. Both inbound and outbound access lists are required between the SCC server and floor equipment, allowing the use of the TCP and UDP ports listed.

Snort Rules

> alert udp any any -> any 12345 (msg:"PROTOCOL-OTHER Pwned piper exploitation attempt, Too small and malformed Translogic packet"; dsize:<21; content:"TLPU"; depth:4; content:"|00 00 00 01|"; distance:4; within:4; reference:cve,2021-37161; reference:url,https://www.armis.com/pwnedPiper; sid:9800002; rev:1;)

General Security Recommendations

Swisslog Healthcare recommends upgrading to the latest software version as soon as available.

Vulnerability Classification

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (NVD - CVSS v3 Calculator (nist.gov)). 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.

Vulnerability CVE-2021-37165

To exploit this vulnerability, an unauthenticated attacker must be on the local network.

CVSS v3.1 Base Score	9.1
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE Reference:	CWE-122, CWE-191

Recommended Actions

1. Swisslog Healthcare recommends upgrading to the latest software version as soon as available.
2. Swisslog Healthcare recommends deploying the described mitigation methods until the updated software version is deployed

Credits

Swisslog Healthcare would like to thank the Armis security research team in reporting this issue in a professional manner.

Support and Contact Information

Product Technical Support

- Phone 24/7 support: 800-396-9666

Report a New Security Finding

- swisslog-healthcare.com/en-us/customer-care/security-information
- Product-Security@Swisslog-Healthcare.com