Armis Discovers 9 Vulnerabilities in Infrastructure Used by 80% of Major Hospitals in North America

Vulnerability Bulletins | Aug 02, 2021, 10:13 AM

Armis researchers have identified nine critical vulnerabilities in one of the leading providers for pneumatic tube systems (PTS) in North America, the Translogic PTS system developed by Swisslog Healthcare.

This Translogic PTS system is used in over 80% of hospitals in North America and has been installed in over 3,000 hospitals worldwide. PTS systems play a crucial role in patient care and are utilized nearly constantly. Dubbed PwnedPiper by Armis researchers, the vulnerabilities allow for complete takeover of the Translogic NexusControl Panel, which powers all current models of Translogic PTS stations that are actively supported by Swisslog Healthcare. Older models that are not currently supported by Swisslog Healthcare are impacted as well.

The Swisslog PTS system is vital to hospital operations as it automates logistics and the transport of materials throughout the hospital via a network of pneumatic tubes. The system is designed so that hospitals can provide better patient care with automated material transport that includes highly-sensitive materials like lab specimens, blood products, pathology lab tests, medications, and more. Prior to the use of PTS systems, hospitals were required to manually transfer the various items, and today, due to their wide adoption, these systems are vital for proper workflow of hospital operations.

These vulnerabilities can enable an unauthenticated attacker to take over Translogic PTS stations and essentially gain complete control over the PTS network of a target hospital. This type of control could enable sophisticated and worrisome ransomware attacks, as well as allow attackers to leak sensitive hospital information.

A high-level description of the discovered vulnerabilities is listed below. All of the vulnerabilities can be triggered by sending unauthenticated network packets, without any user-interaction.

- A hardcoded password vulnerability of user and root accounts, that can be accessed by login to the Telnet server on the Nexus Control Panel, which is enabled by default, and cannot be turned off by native configuration of the system
  - CVE-2021-37163 - Two hardcoded passwords accessible through the Telnet server
- A privilege escalation (PE) vulnerability due to a user script being run by root. By using the hardcoded credentials of the user account, through the telnet server, the user can leverage this PE to gain root access.
  - CVE-2021-37167 - User script run by root can be used for PE

- Four memory corruption bugs in the implementation of the TLP20 protocol as used in the Nexus Control Panel, that can lead to remote-code-execution and denial-of-service. The TLP20 protocol is the control protocol for all Translogic stations.
    - CVE-2021-37161 - Underflow in udpRXThread
    - CVE-2021-37162 - Overflow in sccProcessMsg
    - CVE-2021-37165 - Overflow in hmiProcessMsg
    - CVE-2021-37164 - Off-by-three stack overflow in tcpTxThread
- A denial-of-service vulnerability that is a result of the GUI process on the Nexus Control Panel binding a local service on all interfaces, allowing external connections to hijack its connection. This can allow an attacker to mimic the GUI commands versus the low-level process that controls the Nexus Control Panel, effectively accessing all GUI commands through the network.
    - CVE-2021-37166 - GUI socket Denial of Service
- A design flaw in which firmware upgrades on the Nexus Control Panel are unencrypted, unauthenticated and do not require any cryptographic signature. This is the most severe vulnerability, since it can allow an attacker to gain unauthenticated remote code execution by initiating a firmware update procedure while also maintaining persistence on the device.
    - CVE-2021-37160 - Unauthenticated, unencrypted, unsigned firmware upgrade

Armis reported the vulnerabilities to Swisslog on May 1, 2021 and worked with the developers to create and test a viable patch (v7.2.5.7) for the affected systems, as well as develop alternative mitigation steps for hospitals unable to apply the fix right away.

Recommendations:
While patching the vulnerable Translogic PTS stations (v7.2.5.7) is essential and is urged by the developers and researchers, external mitigations can also be useful for detection and preventing attacks on affected systems.
Below are mitigation steps that can be used to identify and potentially block the discovered vulnerabilities.

1. Block any use of Telnet (port 23) on the Translogic PTS stations (the Telnet service is not required in production)
2. Deploy access control lists (ACLs), in which Translogic PTS components (stations, blowerd, diverters, etc.) are only allowed to communicate with the Translogic central server (SCC).
3. Use the following Snort IDS rule to detect exploitation attempts of CVE-2021-37161, CVE-2021-37162 and CVE-2021-37165:
    - 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;)
4. Use the following Snort IDS rule to detect exploitation attempts of CVE-2021-37164:
    - alert udp any any -> any 12345 (msg:"PROTOCOL-OTHER Pwned piper exploitation attempt, Too large and malformed Translogic packet";dsize:>350; content:"TLPU"; depth:4; reference:cve,2021-37164; reference:url,https://www.armis.com/pwnedPiper; sid:9800001;)

Additionally, hardening the access to sensitive systems such as PTS solutions, through the use of network segmentation, and limiting access to such devices through strict firewall rules are always recommended and should be in use extensively throughout your security environment.

Sources:
Armis: PwnedPiper White Paper: Uncovering Vulnerabilities in Critical Infrastructure of Healthcare Facilities

- See Attached

Armis: PwnedPiper
BleepingComputer: PwnedPiper Critical Bug Set Impacts Major Hospitals in North America
TechRepublic: PwnedPiper Threatens Thousands of Hospitals Worldwide, Patch Your Systems Now
TheRegister: PwnedPiper Vulns Have Potential To Turn Swisslog's PTS Hospital Products Into Swiss Cheese, Says Armis

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
For Questions or Comments: Please email us at toc@h-isac.org

Reference(s)

Bleeping ComputerArmisTech Republic