HC3: Sector Alert

August 3, 2021 TLP: White Report: 202108031200

PwnedPiper Impact on Healthcare

Executive Summary

Nine vulnerabilities (dubbed PwnedPiper) were recently discovered in a brand (Swisslog) of pneumatic tubes – the tube systems within many hospitals and other healthcare organizations which transports small items such as lab samples, blood, tissue or medication from one part of the medical facility to another – which can allow a cyberattacker to compromise and/or disrupt the operations of the system. These vulnerabilities are believed to impact over 3,000 hospitals worldwide, including 80% of all hospitals in North America. All healthcare organizations are urged to review this document and apply the appropriate steps outlined in the mitigation section as needed.

Report

On August 2, 2021, the cybersecurity company Armis released vulnerability research on pneumatic tube systems (PTS) produced by Swisslog. A PTS is a series of tubes, either in a single building or between several buildings that allows people to move small objects around quickly (see picture to the right). In the case of healthcare organizations, PTS are used to transport items such as lab samples, blood, tissue or medication from one part of the medical facility to another. The Armis research revealed that an unauthenticated attacker could gain full control over Swisslog Translogic PTS that are connected to the internet and then compromise the entire tube network of a target hospital. Armis identified nine vulnerabilities (collectively referred to as PwnedPiper) which have CVEs assigned to them and cover issues such as password leakage, remote code execution, denial-of-service, and full device compromise:

A medical professional uses a pneumatic tube (image source: Duke University)

- CVE-2021-37163 - Two hardcoded passwords that are accessible through the Telnet server on the Nexus Control Panel
- CVE-2021-37167 - Privilege escalation vulnerability due to a user script being run by root
- CVE-2021-37161 - Memory corruption bug in the implementation of the TLP2-0 protocol: Underflow in udpRXThread
- CVE-2021-37164 - Memory corruption bug in the implementation of the TLP2-0 protocol: Off-by-three stack overflow in tcpTxThread
- CVE-2021-37165 - Memory corruption bug in the implementation of the TLP2-0 protocol: Overflow in hmiProcessMsg
- CVE-2021-37162 - Memory corruption bug in the implementation of the TLP2-0 protocol: Overflow in sccProcessMsg
- CVE-2021-37166 - GUI socket Denial Of Service
- CVE-2021-37160 - Unauthenticated, unencrypted, unsigned firmware upgrade

Mitigations

As of the publishing of this alert, Swisslog has released fixes for all the Translogic vulnerabilities except one (CVE-

2021-37160), by virtue of their latest software release (v7.2.5.7). Instructions on identifying impacted systems and updating their software can be found on the Swisslog website. These vulnerabilities also affect older IP-connected Translogic stations which are no longer supported by Swisslog; therefore, updates for those systems are not and may not be developed. The Aremis research can be found on their website. HC3 recommends all healthcare organizations, especially hospitals, determine if they own any impacted PTS and, if so, follow the instructions provided on the Swisslog website to ensure they minimize their attack surface as much as possible.

Please contact us at HC3@HHS.gov with any questions about this or any other of our products or services.

References

PwnedPiper critical bug set impacts major hospitals in North America
https://www.bleepingcomputer.com/news/security/pwnedpiper-critical-bug-set-impacts-major-hospitals-in-north-america/

Statement: TransLogic Firmware Vulnerabilities
https://www.swisslog-healthcare.com/en-us/company/news/2021/07/translogic-firmware-vulnerabilities

Armis: PwnedPiper overview
https://www.armis.com/research/pwnedpiper/

Armis: PwnedPiper report
https://info.armis.com/rs/645-PDC-047/images/Armis-PwnedPiper-WP.pdf

PwnedPiper vulns have potential to turn Swisslog's PTS hospital products into Swiss cheese, says Armis
https://www.theregister.com/2021/08/02/pwnedpiper_swisslog_pts/

Critical vulnerabilities may allow attackers to compromise hospitals' pneumatic tube system
https://www.helpnetsecurity.com/2021/08/02/vulnerabilities-pneumatic-tube-system-pwnedpiper/

PwnedPiper threatens thousands of hospitals worldwide, patch your systems now
https://www.techrepublic.com/article/pwnedpiper-threatens-thousands-of-hospitals-worldwide-patch-your-systems-now/

Popular technology that hospitals use to send lab samples is vulnerable, researchers found
https://www.cyberscoop.com/pneumatic-tubes-ransomware-hospitals-swisslogic-armis/

PwnedPiper vulnerabilities impact 80% of major hospitals in North America
https://therecord.media/pwnedpiper-vulnerabilities-impact-80-of-major-hospitals-in-north-america/

PwnedPiper vulns have potential to turn Swisslog's PTS hospital products into Swiss cheese, says Armis
https://www.theregister.com/2021/08/02/pwnedpiper_swisslog_pts/

Basic flaws put pneumatic tube transport systems in hospitals at risk
https://www.csoonline.com/article/3627275/basic-flaws-put-pneumatic-tube-transport-systems-in-hospitals-at-risk.html

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback