Hive Pro

THREAT ADVISORY

Major Hospitals affected by PwnedPiper Vulnerabilities

TA202127

Threat Level White

Publish Date – Aug 3, 2021

Multiple Zero-day vulnerabilities (PwnedPiper) have been found affecting the HMI-3 Control Panel of Swisslog Healthcare's TransLogic Pneumatic Tube Systems (PTS). PTS is a specialized system that uses compressor to transport medical supplies (lab samples, medication, blood products, and other items) through tubes that connect various departments within big hospitals. using tubes that connect different departments inside large hospitals. The medical instrument has been installed in over 3000 hospitals in North America putting all of them at risk. A version 7.2.5.7 of the Nexus Control Panel has been released to eliminate these vulnerabilities.

Vulnerability Details

CVE ID	Vulnerability Description	CWE ID
CVE-2021-37161	A buffer overflow allows an attacker to overwrite an internal queue data structure and can lead to remote code execution.	CWE-122, CWE-191
CVE-2021-37162	If an attacker sends a malformed UDP message, a buffer underflow occurs, leading to an out-of-bounds copy and possible remote code execution.	CWE-122, CWE-191
CVE-2021-37165	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.	CWE-122, CWE-191
CVE-2021-37164	In the tcpTxThread function, the received data is copied to a stack buffer. An off-by-3 condition can occur, resulting in a stack-based buffer overflow.	CWE-122, CWE-121, CWE-787
CVE-2021-37166	When HMI3 starts up, it binds a local service to a TCP port on all interfaces of the device and takes extensive time for the GUI to connect to the TCP socket, allowing the connection to be hijacked by an external attacker.	CWE-284, CWE-400
CVE-2021-37160	There is no firmware validation (e.g., cryptographic signature validation) during a File Upload for a firmware update.	CWE-494
CVE-2021-37163	The device has two user accounts with passwords that are hardcoded.	CWE-259
CVE-2021-37167	A user logged in using the default credentials can gain root access to the device, which provides permissions for all of the functionality of the device.	CWE-250

References

https://www.darkreading.com/vulnerabilities---threats/multiple-zero-day-flaws-discovered-in-popular-hospital-pneumatic-tube-system/d/d-id/1341584
https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20