Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization

This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 recently set out to better understand how well hospitals and other healthcare providers are doing in securing smart infusion pumps, which are network-connected devices that deliver medications and fluids to patients. This topic is of critical concern because security lapses in these devices have the potential to put lives at risk or expose sensitive patient data.

We reviewed crowdsourced data from scans of more than 200,000 infusion pumps on the networks of hospitals and other healthcare organizations using IoT Security for Healthcare from Palo Alto Networks. An alarming 75 percent of infusion pumps scanned had known security gaps that put them at heightened risk of being compromised by attackers. These shortcomings included exposure to one or more of some 40 known cybersecurity vulnerabilities and/or alerts that they had one or more of some 70 other types of known security shortcomings for IoT devices.

One of the most striking findings was that 52 percent of all infusion pumps scanned were susceptible to two known vulnerabilities that were disclosed in

2019 – one with a “critical” severity score and the other with a “high” severity score.

There is already a vast array of information about known vulnerabilities and approaches for securing these devices, thanks to the efforts of medical equipment makers, security researchers, cybersecurity vendors and regulators who have spent the past decade working to better understand cyber risks associated with use of infusion pumps and other connected medical devices. For example, the U.S. Food and Drug Administration (FDA) announced seven recalls for infusion pumps or their components in 2021, and nine other recalls in 2020.

There are also initiatives led by industry and government aimed at standardizing device information and establishing baseline security criteria for manufacturing these devices. Yet the average infusion pump has a life of eight to 10 years, which means the widespread use of legacy equipment has hampered efforts to improve security. Other factors also continue to undermine overall security hygiene – including insufficient use of network segmentation, failure to implement best practices for securing operational processes and insufficient security training for healthcare workers.

Our discovery of security gaps in three out of four infusion pumps that we reviewed highlights the need for the healthcare industry to redouble efforts to protect against known vulnerabilities, while diligently following best practices for infusion pumps and hospital networks.

Healthcare providers are protected against the vulnerabilities discussed here by the Palo Alto Networks IoT Security platform through the identification of managed and unmanaged devices and risks associated with those devices, the application of risk reduction policies and built-in prevention of known threats, as well as detection of and response to unknown threats.

CVEs discussed	CVE-2019-12255, CVE-2019-12264, CVE-2016-9355, CVE-2016-8375, CVE-2020-25165, CVE-2020-12040, CVE-2020-12047, CVE-2020-12045, CVE-2020-12043, CVE-2020-12041
Related Unit 42 topics	IoT devices

Table of Contents

Severity of Infusion Pump Vulnerabilities

Infusion pumps can number in the thousands in a large hospital or clinic, and recalls, whether due to mechanical failure or cybersecurity vulnerability, can be a source of anxiety for supply chain managers, clinical engineers and IT security teams. The at-risk devices must be identified, found and retired or repaired per the instruction of a given recall. An oversight or a miss in any of these areas – whether the devices need repair, maintenance, software patches or updates – can put patient lives or sensitive information at risk.

We recently analyzed more than 200,000 infusion pumps from seven medical device manufacturers using crowdsourced data supplied by customers using Palo Alto Networks IoT Security for Healthcare to see how many and what types of security vulnerabilities these devices have. In this analysis, the Palo Alto Networks IoT Security platform identified over 40 different vulnerabilities and over 70 different security alerts among the devices, with one or more affecting 75% of the infusion pump devices we analyzed. Here we focus on the threats and vulnerabilities we observed most commonly among that group.

The table below identifies the 10 most prevalent vulnerabilities from analysis of the scan data. It lists the CVE number, severity score and percentage of pumps scanned that were susceptible to that vulnerability. 52 percent of the devices we scanned were flagged as being vulnerable to the top two CVEs, which were publicly disclosed in 2019 and have severity scores of “critical” and “high.”

Top 10 Infusion Pump Vulnerabilities and Percentage of Vulnerable Infusion Pumps as Identified by Palo Alto Networks IoT Security

	CVE	Severity (Score)	% of analyzed pumps with CVEs
1	CVE-2019-12255	9.8 (Critical)	52.11%
2	CVE-2019-12264	7.1 (High)	52.11%
3	CVE-2016-9355	5.3 (Medium)	50.39%
4	CVE-2016-8375	4.9 (Medium)	50.39%
5	CVE-2020-25165	7.5 (High)	39.54%
6	CVE-2020-12040	9.8 (Critical)	17.83%
7	CVE-2020-12047	9.8 (Critical)	15.23%
8	CVE-2020-12045	9.8 (Critical)	15.23%
9	CVE-2020-12043	9.8 (Critical)	15.23%
10	CVE-2020-12041	9.8 (Critical)	15.23%

Table 1. The top 10 most prevalent vulnerabilities found in the more than 200,000 infusion pumps we analyzed.

Note: The BD Alaris System vulnerabilities listed in this report were originally disclosed by the manufacturer in 2017, 2019 and 2020, and corresponding bulletins are available on the BD Cybersecurity Trust Center. Links to each bulletin can also be found in Appendix A. BD has made software updates available to remediate these vulnerabilities and encourages customers to update to BD Alaris PCU version 12.1.2, which became available in July 2021.

Types of Vulnerabilities Observed in Infusion Pumps

The most common vulnerabilities we observed that are specific to the infusion systems we studied can be grouped into several categories according to the effects they may have: leakage of sensitive information, unauthorized access and overflow. Other vulnerabilities stem from third-party TCP/IP stacks but can affect the devices and their operating systems.

Leakage of Sensitive Information

We observe that a large number of vulnerabilities in infusion pump systems – and in internet of medical things (IoMT) devices overall – are related to leakage of sensitive information. Devices vulnerable to this type of issue can leak operational information, patient-specific data, or device or network configuration credentials. Attackers looking to exploit these vulnerabilities need varying degrees of access. For example, CVE-2020-12040, which is specific to clear-text communication channels, can be remotely exploited by an attacker via a man-in-the-middle attack to access all the communication information between an infusion pump and a server. On the other hand, CVE-2016-9355 and CVE-2016-8375 can be exploited by someone with physical access to an infusion pump device to gain access to sensitive information – which makes the attack less likely, but still possible for an attacker with specific motivations.

Overflow and Unauthorized Access

Other vulnerabilities related to overflow or incorrect access control can give unauthenticated users an ability to gain access to a device or to send network traffic in a certain pattern that can cause a device to become unresponsive or operate in a way that is not expected – and in healthcare organizations, this can potentially mean causing a disruption to hospital operations and patient care. Also, the possibility of unauthorized access isn't limited to the successful exploitation of vulnerabilities. Continuous use of default credentials, which are readily available online via a simple search, is another major issue in IoT devices in general – since it can give anyone who is in the same hospital network as the medical devices direct access to them.

Vulnerabilities in Third-Party TCP/IP Stacks

Finally, it is not only sufficient to be aware of vulnerabilities in the infusion systems themselves. Many IoMT (and IoT) devices and their operating systems use third-party cross-platform libraries, such as network stacks, which might have vulnerabilities affecting the device in question. For example, for CVE-2019-12255 and CVE 2019-12264, the vulnerabile TCP/IP stack IPNet is a component of the ENEA OS of Alaris Infusion Pumps, thereby making the devices vulnerable.

Common Security Alerts in Infusion Systems

Overall, most of the common security alerts raised on infusion systems indicate avenues of attacks that the device owner should be aware of, for example, via internet connections or via default username and password

usage. On the other hand, with ML-driven continuous monitoring, any anomalous behaviors on infusion systems can quickly identify potential attacks in progress. Flagging devices displaying anomalous behavior or misuse is crucial to identifying zero-days or live attacks on the system.

Below are the security alerts we observed most commonly in the infusion pumps we analyzed.

10 Most Commonly Observed Security Alerts in Infusion Systems by Palo Alto Networks IoT Security		
	Alert Title	Impact and Relevance
1	Excessive count of TCP reset packets sent from unestablished connections	A large number of reset packets sent from connections outside the local network can indicate a continuous attempt at a connection to an unauthorized destination, which could indicate anomalous behavior on the device.
2	Invalid User Agent string (garbage values) observed in an HTTP request in IoMT device	Garbage values in the User-Agent string can indicate suspicious behavior. This means that the network connection between the infusion system and the corresponding destination should be monitored more closely.
3	Unencrypted sensitive login information observed in an HTTP request	Sensitive information via HTTP (which is a non-encrypted protocol) can be easily monitored by a malicious actor and can leak information related to device/patients.
4	Manufacturer factory default username and password in inbound HTTP login	Use of factory default credentials to log in to a device via HTTP is a serious security concern. These credentials can be easily found online or in manuals and anyone can access them.
5	Suspicious (high and not commonly observed) port number in network traffic	Anomalous port numbers and counts observed in incoming and outgoing traffic in the infusion system. Such anomalous behavior indicates that the device should be more closely monitored.
6	Unsecured outbound HTTP connections from IoMT device to the internet	Outbound connections to the internet (outside the local network) via HTTP (which is non-encrypted) should be avoided for all infusion systems. Communication should be limited to devices inside the hospital network/specific medical VLAN.
7	FTP anonymous login (without specific	Anonymous login without proper credentials can indicate malicious behavior, and the device should be flagged.

	username/password) via local network	
8	Manufacturer factory default username and password in the inbound FTP login	As observed for HTTP, factory default credentials for FTP are a similar security no-no.
9	Unsecure outbound FTP connections from IoMT device to the internet	Similar to outbound HTTP connections from medical devices to the internet, FTP connections outside the hospital network could make the device susceptible to attacks.
10	Unsecure HTTP service hosted on the IoMT device	Hosting an HTTP service on an infusion system, which is a mission-critical medical device, as well as holding sensitive data, makes the device prone to security attacks.

Table 2. The top 10 most prevalent security alerts found in the more than 200,000 infusion pumps we analyzed.

Proactively Secure Your Infusion Pumps

For healthcare providers, keeping vulnerable IoMT devices safe from known and unknown threats goes beyond device identification and alerting. The sheer volume of devices in the healthcare environment makes an alert-only approach risky and impractical. In addition, alert-only solutions require integration with third-party systems for prevention adding to the complexity of deploying and managing these systems over time. Healthcare security teams require IoT security technology with built-in prevention that secures even unmanaged devices.

The pervasiveness of the threats, the volume of devices in service, and the lack of visibility into device risks and behavior combine to make the security challenges seem insurmountable. Here's the good news: With the right strategy and the right security technology, healthcare IT and clinical engineering teams can get the visibility they need to manage and secure all IoMT devices and ensure patient safety.

Here are some key capabilities to consider when evaluating IoMT security strategies and technologies for healthcare.

1. **Accurate discovery and inventory:** Teams must be enabled to quickly discover, locate and assess utilization of all infusion pumps, including mobile and rental equipment. The discovery of infusion pumps supports accurate inventory that can also be shared with asset management or

computerized maintenance management system (CMMS) solutions like ServiceNow. Utilization insights can help with procurement planning and eliminating costly underutilized rental equipment. A location feature comes in handy when planning preventive maintenance or manually applying remediation of an issue.

2. **Holistic risk assessment:** Holistic risk assessment helps security teams proactively find vulnerabilities and identify compliance gaps. A system capable of delivering machine learning-driven insights can help establish a behavior baseline and provide a deep risk assessment. This could include watching for threat indicators (e.g., an abnormal connection between devices or the presence of malicious files. It could also mean monitoring for issues such as default passwords, end of life operating systems, apps or devices, and obsolete protocols. It's also important to monitor CVEs and assess them in context, taking account of additional factors such as FDA recalls, MDS2 information, ePHI information, vendor patching information, patch level and so on. Finally, a risk assessment strategy can be strengthened by extended capabilities achieved through integrations with third-party vulnerability management systems such as Qualys, Rapid 7 and Tenable to scan for additional vulnerabilities in infusion pumps.
3. **Apply risk reduction policies:** Real-time risk monitoring, reporting and alerting are crucial for organizations to proactively reduce IoMT risk. Consistent profiling of device activity and behavior yields data that can be accurately converted into risk-based Zero Trust policy recommendations. This approach enables security teams to confidently allow only trusted behavior, and if necessary, segment infusion pumps from other IT and medical devices to reduce attack radius. For example, as mission-critical devices supporting the lives of patients, such devices should have their own isolated VLANs for communicating with a server and clinical workstations – outbound traffic from such devices can be a real cause for concern, as it could indicate exfiltration of sensitive information.
4. **Prevent Threats:** The diverse nature of IoMT devices will require actionable insights into detection and prevention of known threats against infusion pump devices for a swift response for threat mitigation. Built-in prevention capabilities help block known targeted IoT malware, spyware and exploits, preventing the use of DNS for C2, and stopping access to bad URLs or malicious websites to help prevent the loss of sensitive data.

Palo Alto Networks has been working with healthcare customers closely to help narrow security and compliance gaps across the health system.

Conclusion

Among the 200,000 infusion pumps we studied, 75% were vulnerable to at least one vulnerability or threw up at least one security alert. While some of these vulnerabilities and alerts may be impractical for attackers to take advantage of unless physically present in an organization, all represent a potential risk to the general security of healthcare organizations and the safety of patients – particularly in situations in which threat actors may be motivated to put extra resources into attacking a target.

With attack surfaces widening and attack vectors becoming more refined than ever before, now's the time for healthcare organizations to define medical device security with a new level of sophistication. To successfully implement secure clinical and device workflow management that is scalable, yet practical to maintain and enforce, the methodology should also alleviate the escalating operational burdens of securing and managing medical devices for both network security and clinical support teams.

The IoT Security platform protects customers from these security risks by accurately identifying devices on the network; assessing risk by evaluating device profiles for vulnerabilities, exposures or security advisories; detecting anomalies with ML-driven continuous monitoring; and enabling built-in prevention for attacks exploiting these vulnerabilities, including known and unknown threats, with automated Zero Trust policy recommendations and enforcement.

Additional Resources

Windows XP, Server 2003 Source Cloud Leak Leaves IoT, OT Devices Vulnerable
The Healthcare CISO's Guide to IoMT Security
Zero Trust Security Guide for Healthcare

Appendix A

BD published product security bulletins for the vulnerabilities listed in this report, which include:

CVE	Manufacturer's Vulnerability Disclosure	Date Published
CVE-2019-12255	Interpeak IPNET TCP/IP stack vulnerability	Oct. 1, 2019
CVE-2019-12264	Interpeak IPNET TCP/IP stack vulnerability	Oct. 1, 2019
CVE-2016-9355	Potential Physical Access to Wireless Credentials Alaris™ PC Unit (PCU) (model 8000)	Feb. 6, 2017
	Potential Physical Access to Wireless Credentials Alaris PC Unit (PCU) (model 8015)	January 2017
		Update Oct. 11, 2017
		Update March 16, 2021
CVE-2016-8375	Potential Physical Access to Wireless Credentials Alaris™ PC Unit (PCU) (model 8000)	Feb. 6, 2017
	Potential Physical Access to Wireless Credentials Alaris PC Unit (PCU) (model 8015)	January 2017
		Update Oct. 11, 2017
		Update March 16, 2021
CVE-2020-25165	BD Alaris™ 8015 PC Unit and BD Alaris™ Systems Manager Network Session Vulnerability	Nov. 12, 2020

Other vendors may also have published advisories on other mentioned vulnerabilities.