Max-Severity Bug in Infusion Pump Gateway Puts Lives at Risk

Author: Tara Seals
June 13, 2019
threatpost.com/critical-bug-infusion-pump-lives-at-risk/145660/

The critical bug in a connected medical device can allow an attacker to remotely manipulate hospital pumps, either to withhold meds or dispense too much.

Researchers have disclosed two separate vulnerabilities within the Becton Dickinson Alaris Gateway Workstation for medical infusion pumps in hospitals, one carrying a critical rating of 10 out of 10 on the CVSS v.3 severity scale.

Alaris Gateway Workstations power, monitor and control infusion pumps, which are a common medical device used in hospital wards and ICUs, automatically dispensing a drug directly to a patient over time. Infusion pumps can deliver insulin, painkillers or other medicines that require intermittent or continuous dosing. In many cases, a patient under treatment has multiple infusion pumps running side-by-side, dispensing different drugs, connected to a single medical gateway.

The critical vulnerability allows hackers to remotely install unauthorized firmware in the Alaris Gateway and adjust specific commands on the infusion pump, including altering the doses of drugs being administered or preventing them from being administered at all – which could have obvious patient safety consequences.

That bug also has a low complexity score – meaning that it's relatively simple to exploit the vulnerability, according to CyberMDX, which is issued the advisory in consultation with ICS-CERT, on Thursday.

Elad Luz, head of research at CyberMDX, told Threatpost that the consequences of exploitation could be dire.

"If remotely compromised, a hacker can alter infusion rates, increasing dosage," he said. "It also would be possible to stop infusion. Both scenarios would have a direct impact on a patient's health. In addition, alerts can be silenced, thereby rendering built-in safety measures useless."

He also said that denial of service could be in the offing: “High impacts to system and data integrity and availability exist as complete or partial disabling of the gateway is possible.”

The good news is that so far, there is no evidence of in-the-wild exploitation.

“An interesting thing to note here is how innocent looking the device is – it looks like a stand that simply distributes power and connection to the docking pumps, however turns out it plays quite a critical role and runs a WindowsCE operating system,” Luz told Threatpost.

The second vulnerability (CVE-2019-10962), which is a medium-rated flaw with a score of 7.5 out 10, impacts the Web Browser User Interface on the Alaris Gateway Workstation. If exploited, the vulnerability will allow hackers with knowledge of the IP address to gain access to device monitoring, event logs and configuration.

Following responsible disclosure guidelines, CyberMDX contacted device manufacturer Becton Dickinson, which conducted its own testing and confirmed the vulnerabilities.

“They will be issuing a security bulletin to customers, along with mitigation and compensating control recommendations,” Luz told Threatpost.

Exploitation and Mitigation

In order to exploit the critical vulnerability, an attacker would need to compromise a hospital network and be able to update and manipulate a CAB file, which stores files in an archived library and utilizes a proper format for Windows CE, according to CyberMDX.

“The hackers would also need to create an executable with custom code that can run in the Windows CE environment, understand how the communication protocols are utilized within the product and create an installer for the CAB file, with settings required to run the program,” the firm noted in its advisory.

Compromising hospital networks is not that challenging of a process, according to researchers, and exploitation after doing so, Luz told Threatpost, is “quite easy.”

“It simply required crafting a cab file with WinCE executables, some info about the internal file system and info about transferring the update over SMB,” he noted.

Hospitals can reduce their risk by blocking the SMB protocol, segregating their VLAN network and ensuring that only appropriate associates have access to the customer network.

To patch both vulnerabilities, hospital admins can update to the latest firmware version, 1.3.2 or 1.6.1, to patch the flaw.

Hospitals: Still Struggling with Connected Devices

One of the weakest links within clinical networks are connected medical devices, as various vulnerabilities have shown over time. For instance, last year a slew of devices from the same vendor, BD, were found to be vulnerable to the infamous KRACK key-reinstallation attack, potentially enabling hackers to change and exfiltrate patient records.

Part of the problem in healthcare environments when it comes to addressing bugs is a lack of resources, both human and software-related. “Healthcare providers rely on connected medical devices for their clinic workflows

and life-saving treatments, however, unlike other IT assets, connected medical devices are extremely vulnerable," Luz told Threatpost. "Healthcare organizations are concerned about non-secure medical devices, yet most of them lack proper solutions in their toolbox to address the problem."

Another issue is that many hospital environments are running legacy systems, with a wide range of operating systems and device-specific communication protocols. At DEF CON 2018 for instance, researchers at McAfee found that the aging RWHAT protocol, used by medical devices to monitor a patient's condition and vital signs, and communicate with nurses' stations, can be easily subverted. It has a weakness that allows data on the patient's condition to be modified by an attacker in real-time, to provide false information to medical personnel.

The ramifications are profound; false information could lead a doctor to prescribe medication that the patient doesn't need; or, a patient could be thought to be peacefully resting, when in fact they are under cardiac arrest.

Gaining visibility over the environment can go a long way to mitigating these kinds of risk, Luz pointed out.

"Unlike other critical IT assets, connected medical devices are hardly visible in their native IT control systems," he told Threatpost. "The IT teams often cannot even tell how many medical devices are connected, their type, and they lack critical insight of the devices cybersecurity risk status, threats and vulnerabilities. Even more shocking, most hospitals lack the visibility to whether medical devices have been hacked."

He added, "It starts with inventory – identifying and classifying every connected device. The next step is to properly plan risk analysis, risk mitigation and incident-response plans. There are no shortcuts here."