Widely used medical infusion pump can be remotely hijacked

17 JUN 2019 0

Security threats, Vulnerability

Previous: Monday review – the ho... Next: I'd like to add you to my prof...

by Lisa Vaas

Researchers have found two security vulnerabilities, one severe, in Becton Dickson (BD) infusion pumps: the devices used in hospitals for supplying power and network connectivity to multiple infusion and syringe pumps that deliver fluids, including intravenous fluids, painkillers and medications such as insulin.

Such pumps are often hooked up to a central monitoring station so that hospital staff can check on multiple patients at the same time.

The flaws, in BD's Alaris Gateway Workstation (AGW), were discovered by the healthcare cybersecurity firm CyberMDX in September 2018. The firm's researchers said on Thursday that one of the security flaws – the most critical, according to an advisory issued by the Department of Homeland Security (DHS), also on

Thursday – could allow the devices to be remotely hijacked and controlled.

The researchers said that the exploit could be carried out by...

> *... anyone who gains access to the hospital's internal network. Files transferred via the update are copied straight to the internal memory and allowed to override existing files.*

The vulnerable part of the pumps is the firmware in the onboard computer, which powers, monitors and controls the infusion pumps. The pumps run on Windows CE, which is Microsoft's operating system for embedded devices and devices with minimal memory. That operating system later came to be known as Windows Embedded Compact.

No exploits to date

On Thursday, Becton Dickson said in an advisory that there haven't been any reported exploits of the critical vulnerability.

Nor does it affect the latest firmware version 1.3.2, nor version 1.6.1. Only older software versions for 2.3.6 – which was released in 2006 – and below are affected, the company said.

The affected products aren't sold or used in the US. They are, however, widespread in Asia and Europe.

The silver lining

Also on the plus side is the fact that exploiting the more critical of the two vulnerabilities takes a good amount of know-how, as BD outlined in a security bulletin published on Thursday.

> *In order to access this vulnerability, an attacker would need to gain access to a hospital network, have intimate knowledge of the product, be able to update and manipulate a CAB file which stores files in an archived library and utilizes a proper format for Windows CE.*

Attacker could alter infusion rate or completely stop pump

In the worst-case scenario, if an attacker were able to pull that off, they could then adjust commands on the pump – including adjusting the infusion rate on some specific, mounted infusion pumps that BD listed in its advisory, or, as DHS explained, turning off the pump completely.

An attacker could, in other words, cause a patient to get far too much or too little of a medication, with a potentially lethal outcome.

Beyond exploit of that critical vulnerability, an attacker could also exploit a vulnerability on the AGW. In order to do that, BD said the attacker would need to...

> *... create an executable with custom code that can run in the Windows CE environment, understand how the*

> *internal communication protocols are utilized within the product and create a specific installer for the CAB file, with settings required to run the program.*

This second vulnerability could allow an attacker to gain access to the workstation's monitoring and configuration interfaces through the web browser. BD called it "difficult to exploit."

BD said that no patient information is stored on the interface "by default" but that a successful exploit could allow an attacker to view information including event logs and to change a workstation's network configuration.

The not-so-silver lining

On the flip side of the silver lining, the critical vulnerability, which allows for remote access without any steps having to be taken on the part of the hospital staff and which is being tracked as ICS-CERT Advisory CVE-2019-10959 – has been given the maximum score on the vulnerability scale: CVSS 10, due to the fact that no authentication is required to access the device and upload malicious files.

DHS noted that these vulnerabilities mark the fourth time that it's sent out cybersecurity notices about BD's Alaris line of products. One of the prior vulnerabilities received almost as high a score as the new firmware problem, DHS said.

One such was a slew of medical devices found to be vulnerable to KRACK Wi-Fi attacks last year.

KRACK, or, more properly, the KRACK Attacks, stands for Key Reinstallation Attack(s). They work by exploiting a flaw in WPA and WPA2 protocol encryption, which these days covers most wireless access points where encryption has been turned on.

What to do?

BD is telling users to mitigate the firmware threat by blocking a client-server communication protocol used for sharing access to files. It said that customers should...

- Utilize the latest firmware to eliminate the vulnerability.
- Block the SMB protocol.
- Segregate their VLAN network.
- Ensure that only appropriate associates have access to the customer network.

BD will share details about an additional response within the coming two months.