

Memo

|  |  |
| --- | --- |
| To: | CISO Chris Bailey |
| From: | Tri D Ho |
| Date: | July 5th, 2022 |
| Re: | Vulnerabilities in medical devices |

The purpose of this memo is to inform you and the board of vulnerabilities in medical devices that can connect to the Internet via Wi-fi. Includes here are two examples that I found worth noticing and can serve as a basis for research in formulating security standards and protocols.

**Device 1: Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Version 1.1, 1.5, 1.6**

* The affected models are versions 1.1, 1.5, and 1.6 of the Medfusion 4000 Wireless Syringe Infusion Pump. These are syringe infusion pumps that deliver small doses of medications in acute care settings. According to the Cybersecurity & Infrastructure Security Agency (CISA), these devices are deployed worldwide across the Healthcare and Public Health sectors by Smith Medical. The vulnerabilities make it possible for an attacker to compromise the communication module and the therapeutic module of the pump (2017).
* CVE-2017-12718. Description: A Classic Buffer Overflow issue was discovered in **Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Version 1.1, 1.5,** and **1.6**. A third-party component used in the pump does not verify input buffer size prior to copying, leading to a buffer overflow, allowing remote code execution on the target device. The pump receives the potentially malicious input infrequently and under certain conditions, increasing the difficulty of exploitation (CVE, 2017).
* To mitigate some of the risk factors, Smith Medical released the updated version 1.6.1 with patches for this problem. Additionally, the manufacturer also recommends a series of defensive measures such as:

1. Using strong passwords
2. Monitoring network activities
3. Assign static IP addresses when in usage.
4. Most importantly, Smith Medical recommends the user segment the network so that the device is on a separate network from the remaining clinical information and technology structure (CISA, 2017).

* My first recommendation to the Northwest Shelbyville Regional Hospital (NSRH) is to avoid using the device completely. The Medfusion 4000 device requires constant monitoring when connecting to the internet. Even though the device can operate offline, it would require manual input, and check from the medical staff. In the event of NSRH already purchase these devices and return is not possible, there are several methods we can use to make this device more secure:

1. Make sure the device comes in with the updated version 1.6.1.
2. Disconnecting the device when not in use. The pump can run when offline. It will require the medical staff to input the data, however.
3. Use VPN when the pump must be connected to the Internet and make sure Port 20/FTP, Port 21/FTP, and Port 23/Telnet are closed (CISA, 2017).

**Device 2: Medtronic Paradigm wireless insulin pumps 512, 522, 712,** and **722**

* A DOS attack was performed on the wireless Medtronic Paradigm wireless insulin pump. The attacker is an IT professional who performs the attack on his own device as an experiment. The device’s primary function is to measure/display the wearer’s glucose level. It will then release doses of insulin to the body whenever the glucose level is too high. With the assistance of a $10 radio and an oscilloscope, the attacker can alter the glucose reading from half a mile away, which in turn can make the insulin pump stop all insulin or over-releasing the insulin and put the patient’s life in great danger.
* CVE CVE-2011-3386. Description: Unspecified vulnerability in **Medtronic Paradigm wireless insulin pumps 512, 522, 712,** and **722** allows remote attackers to modify the delivery of an insulin bolus dose and cause a denial of service (adverse human health effects) via unspecified vectors involving wireless communications and knowledge of the device's serial number, as demonstrated by Jerome Radcliffe at the Black Hat USA conference in August 2011 (CVE, 2011).
* There is no known solution or resolution to this vulnerability according to IBM Security (2011). Additionally, the manufacturer argues that the hacking was done by an IT professional and therefore unlikely can be replicated by the public (CVE, 2011).
* My recommendation is to avoid this device at all costs. The hacker that performs the DOS attack used a $10 radio and an oscilloscope to analyze the bit (Hanselman, 2011). As of this moment, there is solution or remedies that can be applied to mitigate the risk (IBM Security, 2011). Furthermore, Medtronic, the manufacturer does not provide any additional guidance or indication of troubleshooting this problem.

References

Common Vulnerabilities and Exposures (2011). CVE-2011-3386​. CVE. Retrieved July 5, 2022, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3386>

Cybersecurity & Infrastructure Security Agency. (2017, September 7 ). *Smiths medical medfusion 4000 wireless syringe infusion pump vulnerabilities (update 2017, December 12) | CISA*. https://www.cisa.gov. Retrieved July 5, 2022, from <https://www.cisa.gov/uscert/ics/advisories/ICSMA-17-250-02A>

Common Vulnerabilities and Exposures (2017). CVE-2017-12718​. CVE. Retrieved July 5, 2022, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12718>

Hanselman, S. (2011, August 5). *Hackers can kill diabetics with insulin pumps from a half mile away - Um, no. facts vs. journalistic fear mongering*. Scott Hanselman. Retrieved July 5, 2022, from <https://www.hanselman.com/blog/hackers-can-kill-diabetics-with-insulin-pumps-from-a-half-mile-away-um-no-facts-vs-journalistic-fear-mongering>

IBM security. (2011, August 4). *Medtronic Paradigm wireless insulin pump denial of service CVE-2011-3386 Vulnerability Report*. <https://exchange.xforce.ibmcloud.com>. Retrieved July 5, 2022, from <https://exchange.xforce.ibmcloud.com/vulnerabilities/69643>