To: Northwell Shelbyville Regional Hospital

From: Alvin Sarkadi

Date: 1/31/2022

Re: Security risks at N.S.R.H

This document will discuss the common vulnerabilities and exploitations of devices that are important to our community. Wireless technology is a growing phenomenon that many are interested in. Different types of wireless technologies are used everyday in hospitals. It is important that we secure these devices for the safety of the staff, the patients, and the organization. Additionally, like wireless technology, hacking is also a growing phenomenon. Data breaches, ransomware, viruses, SQL injections, are a common threat in public and private networks, especially hospital networks. It is important to address such vulnerabilities to secure the organization's data. Having a high vulnerability exploited within one of the organizations networks would be significantly harmful to the organizations data. Staff and patient credentials, medical records, Insurance, social security numbers, and credit card numbers could be stolen, sold, or used as ransom.

Device 1: Insulet Omnipod Insulin Management System insulin pump

CVE-2020-10627:

- This is an insulin management device. The device is capable of numerous tasks such as taking vitals, advisory alarms, hazard alarms, emergency alarms, low or high blood glucose levels, rapid heart rate, and produces proper insulin dosages. This device is for individuals suffering from diabetes, the company notes that controlling the management 'Pod' is significantly more convenient then using an insulin syringe.
- The company also highly recommends using the Pod strictly through physically accessing the Omnipod system. They insist that using other sources such as computers or tablets to monitor Omnipod, can cause 'differences' in insulin dosage. This was found on page 13 of their user guide. (I assume this warning is associated with the current CVE being discussed.)

- CVE-2020-10627 Description: Omnipod's wireless RF communication protocol does not implement security or any sense of authentication. This is for product ID's: 19191 and 40160. An attacker can intercept traffic and controls to the device, including insulin

dosage and delivery. This is a major problem because wireless devices should always have the most up to date authentication and security. Especially, if the device is for public/daily use. This is the only known explained vulnerability, however, I imagine this vulnerability is extremely prone to remote access. (Full control over the device by the attacker.) I highly recommend recalling any Insulet Omnipod Insulin Management System insulin pumps (Product ID: 19191 and 40160.) I would advise doctors and physicians, nutritionists, to re-assess treatment for patients with Insulet Omnipod 19191, 40160. My recommendation is to hire or contract a third-party reliable penetration tester to maintain and secure all networks that can interfere with the Hospital. The current information security team needs to reassess how they can access these vulnerabilities easier. There is other HIPAA approved Insulin management systems that should be considered. Upon further investigation, the NVD (National Vulnerability Database) created a detailed article based on this CVE. The NVD uses a security severity score based on (1-10) called CVSS. CVSS is a string vector that explains to an analysist what is wrong. Such as, integrity, privileges required, confidentiality and more. The CVSS measured the severity of this vulnerability as 8.1, labeled 'high.' The NVD also uses third-party advisory from the Cybersecurity & Infrastructure Security Agency. Due to the severity, the Cybersecurity & Infrastructure Security Agency also created an Advisory / Article regarding Insulet Omnipod. Stating the following: "1. EXECUTIVE SUMMARY CVSS v3 7.3

- ATTENTION: Low skill level to exploit/public exploits are known for this vulnerability
- Vendor: Insulet
- Equipment**:** Omnipod Insulin Management System
- Vulnerability: Improper Access Control
- 2. RISK EVALUATION
- Successful exploitation of this vulnerability may allow an attacker to gain access to the affected products to intercept, modify, or interfere with the wireless RF (radio frequency) communications to or from the product. This may allow attackers to read sensitive data, change pump settings, or control insulin delivery." (ICS-CERT, 2020.)

In conclusion, considering this information, I highly suggest doctors, patients, and staff to discontinue using and recommending Omnipod Insulin Management System.

Device 2: CVE – 2022 – 23857:

Navidrome an open-source streaming service for audio such as music, podcasts, or radio. Like other streaming services, Navidrome can create libraries and playlists based on a person's likings and store them on a smartphone (Android and IOS). It seems the website is targeted to those who are familiar with open-source audio possession and streaming. The service highlights notable features such as being open source, allowing third parties to contribute through their pull request feature on GitHub, efficient streaming through IOS and Android devices, including resource limited devices such as a Raspberry Pi. Navidrome includes a UI like Spotify and other popular audio streaming services.

CVE – 2022 – 23857:

Before Navidrome's 0.47.5 update, user's using the Navidrome UI could be targeted in a SQL injection attack, specifically, when the user is making a 'Smart playlist.' This attack makes it very easy for hackers to steal credentials or other files stored on the database. Based on this factor, I highly recommend all staff to always update their audio streaming services automatically on their smartphones, computers, and tablets. Alternatively, I also recommend staff to use safe closed source alternatives that are not as vulnerable to breaches, such as Spotify, while at work connected to hospital networks. Furthermore, since this attack, their open-source repository is updated every 1-2 days, I would still only recommend this software outside the range of the hospital networks since it is an open-source project.

References -

ICS-CERT. (2021, December 1). *CVE-2020-10627 Detail*. NVD. Retrieved February 3, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2020-10627

CISA. (2021). *ICS Medical Advisory (ICSMA-20-079-01)*. ICS Medical Advisory . Retrieved February 3, 2022, from https://www.cisa.gov/uscert/ics/advisories/icsma-20-079-01

CVE - CVE-2022-23857. (2022). Mitre.org. Retrieved February 3, 2022, from

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23857

CVE - CVE-2020-10627. (2020). Mitre.org. Retrieved February 3, 2022 from,

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10627

Navidrome. (2021). *Navidrome*. Navidrome. Retrieved February 3, 2022 from,

https://www.navidrome.org/#td-block-1

Omnipod (2020). Omnipod Insulin Management User Guide. Retrieved February 3, 2022 from

https://www.omnipod.com/sites/default/files/2021-04/Omnipod-System_User-Guide_English.pdf

NVD - CVE-2022-23857. (2022). Nist.gov. Retrieved February 3, 2022 from https://nvd.nist.gov/vuln/detail/CVE-2022-23857

NVD - CVE-2020-10627. (2020). Nist.gov. Retrieved February 3, 2022 from https://nvd.nist.gov/vuln/detail/CVE-2020-10627