# Assessing Medical Device Vulnerabilities on the Internet of Things

Emma McMahon, Ryan Williams, Malaka El, Sagar Samtani, Mark Patton, Hsinchun Chen
Department of Management Information Systems
The University of Arizona
Tucson, AZ 85721
{mcmahone, ryanwilliams12, msel, sagars, mpatton}@email.arizona.edu, hchen@eller.arizona.edu

***Abstract*—Internet enabled medical devices offer patients with a level of convenience. In recent years, the healthcare industry has seen a surge in the number of cyber-attacks. Given the potentially fatal impact of a compromised medical device, this study aims to identify vulnerabilities of medical devices. Our approach uses Shodan to obtain a large collection of IP addresses that will be passed through Nessus to verify if any vulnerabilities exist. We determined some devices manufactured by primary vendors such as Omron Corporation, FORA, Roche, and Bionet contain serious vulnerabilities such as Dropbear SSH Server and MS17-010. These allow remote execution of code and authentication bypassing potentially giving attackers control of their systems.**

***Keywords—medical devices; health; vulnerability assessment; Shodan; Nessus; IoT***

## I. Introduction

Recent years have seen a surge of cybersecurity incidents within the healthcare industry. Major organizations such as Anthem, Premera Blue Cross, and Excellus have seen malicious hackers steal millions of records from their systems [1-3]. However, health data records are not the only target in the healthcare domain. The emergence of Internet of Things (IoT) technologies have given rise to Internet enabled insulin pumps, pacemakers, MRI machines and other medical devices.

The American Hospital Association (AHA) has identified that Internet enabled medical devices significantly enhance customer care and efficiency [4]. However, they also note that medical devices are more susceptible to cyber-attacks than ever before. Researchers have found that communications to and from pacemakers could be intercepted or altered, potentially causing injuries or even death [5]. Additionally, Johnson & Johnson in 2016 discovered a vulnerability in one of their insulin pumps, that when exploited, would deliver excess amounts of insulin to the patient [6]. Such situations motivate the need to identify vulnerabilities within medical devices prior to exploitation.

One tool that can aid in identifying potentially vulnerable Internet enabled medical devices is Shodan, a search engine for the IoT. Shodan allows users to access its billion-record database with a web interface and/or API. Figure 1 illustrates how a user can search for and access a medical device manufactured by Omron Corporation, a major medical device vendor.

Given the potentially severe consequences of exploiting Internet enabled medical devices, this study aims to identify the vulnerabilities of Internet enabled medical devices that are accessible on Shodan. Specifically, we utilize Shodan's web API to gather thousands of devices from major medical device vendors coupled with Nessus, a state-of-the-art vulnerability assessment tool, to assess the vulnerabilities of collected devices.

The remainder of this paper is organized as follows. First, we review literature of healthcare devices and vulnerability assessments. Second, we describe our research testbed. Subsequently, we summarize the key findings and results. Finally, we suggest future directions and conclude our research.

## II. Literature Review

We reviewed two areas of literature: (1) networked healthcare devices to understand what types of medical instruments are susceptible to cyber-attacks and (2) vulnerability assessment to determine the standard approaches for identifying device vulnerabilities.

### A. Medical Device Security Concerns

Lake et al., noted that "the chances of security breaches increase in direct proportion to the 'degree of connectivity'" [7]. Today, Internet enabled medical devices have drastically

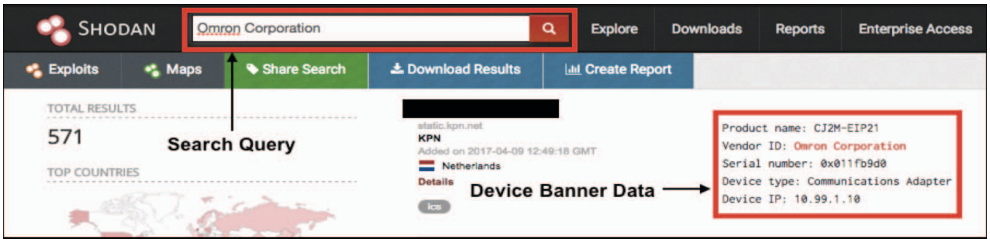


Figure 1. Shodan Results for Omron Corporation Search

improved the quality of healthcare services [5, 7]. Despite numerous benefits, Sametinger et al. noted that Internet capabilities in medical devices allows attackers to obtain sensitive information and infect devices with malware, thus endangering human lives [8]. Many implantable devices such as pacemakers, neurostimulators, implantable cardiac defibrillators (ICDs), and drug delivery systems are prime targets for cyber-attacks [9]. To address the growing concern of cybersecurity in medical devices, the Food and Drug Administration (FDA) has created cybersecurity guidelines for three medical device classes (table 1) before devices are introduced to the market [10].

TABLE I. MEDICAL DEVICE CLASSES

| Medical Device Class | Attributes | Example Devices |
|---|---|---|
| Class I | Common, low risk, low complexity | Lancet, Dental Floss |
| Class II | More complex, greater risk to patient, partially implanted | Syringe, Insulin Pump, BGM |
| Class III | Fully implanted, greater risk, regulate body functions | Artificial Pancreas, CGM, Replacement Heart Valves |

Cybersecurity concerns generally revolve around class II and III devices [8]. For example, Jay Radcliffe hacked into an insulin pump, a Class II device, using the serial number and could send commands to or disable the device [11]. For diabetics reliant on properly functioning insulin pumps, this could be devastating. Such an example motivates assessing the vulnerabilities of other connected medical devices to mitigate potentially severe attacks.

### *B. Vulnerability Assessment Approaches*

Vulnerability assessments aim to provide organizations with knowledge of systems susceptible to cyber-attacks. There are four steps to conducting a vulnerability assessment: (1) define assessment scope, (2) utilize software to identify vulnerabilities, (3) analyze the software-generated reports, and (4) attempt to exploit the system using the known vulnerabilities [11]. Past scholars have utilized this procedure when conducting vulnerability assessments on SCADA systems and generic IoT systems [12, 13].

Today, there are many vulnerability assessment tools such as Burp Suite, Nessus, Qualys, and Nexpose [14]. Among these, Nessus has been identified as the most ideal for large-scale vulnerability assessments for several reasons [12, 15]. First, it offers the most diverse set of plugins for assessing a broad range of technology such as SCADA devices, web applications, and Window/Linux systems. Second, Nessus was designed to scan networks with thousands of devices. Finally, Nessus categorizes vulnerabilities into five risk categories (‘Critical’, ‘High’, ‘Medium’, ‘Low’, and ‘None’) based on the industry standard Common Vulnerability Scoring System (CVSS).

### *C. Research Gaps and Questions*

Despite the importance of identifying vulnerabilities of Internet enabled medical devices and the maturity of vulnerability assessment approaches, we were unable to find any study focusing on discovering the vulnerabilities of such devices. To address this gap, we pose the following research question for study:

- What vulnerabilities are medical devices Internet accessible via a public IP address susceptible to?

## III. RESEARCH DESIGN AND TESTBED

Our research design (Figure 2) has three major components: device identification, vulnerability assessment, and results evaluation.

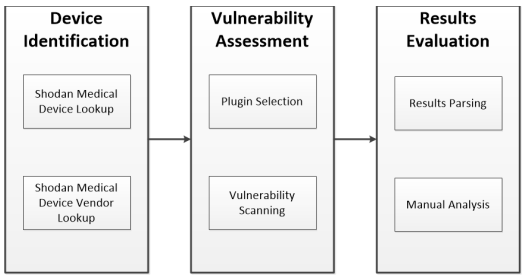


Figure 2. Research Design

The device identification component identifies Internet enabled medical devices on Shodan. Similar to past work, we leverage a set of medical device (e.g., insulin pumps, MRI scanners, pacemakers, glucose monitors) and vendor specific (e.g., Omron Corporation, Welch Allyn) keywords to identify 17,292 medical device IP’s with the Shodan API [12, 13].

After identifying relevant IP addresses, they were passed to Nessus using Python. We configured Nessus to identify outdated operating systems, web vulnerabilities, and test for default credentials. We avoided port scans because of the potential harm to devices. All scans completed in 22 hours on a virtualized machine with 36 cores, 60 GB of RAM, and 100 GB space of SSD. After scanning, all results were parsed into our database for manual evaluation.

## IV. RESULTS AND DISCUSSIONS

Our vulnerability assessment identified 1,604/16,078 (9.97%) of devices with vulnerabilities. Each device can have multiple vulnerabilities. Overall, there were 3,964 vulnerabilities in 1,604 devices. 345 devices had ‘Critical’ vulnerabilities, 411 with ‘High’, 1,468 with ‘Medium’, and 1,740 with ‘Low’ vulnerabilities. Table II summarizes the three most common vulnerabilities for the ‘Critical’ and ‘High’ thresholds. We also detail selected devices, vendors, and products afflicted by the vulnerabilities.

The most common vulnerability found at the critical level was the Dropbear SSH Server. Attackers can exploit this vulnerability to execute malicious code on the database client potentially disclosing sensitive information held on the database. This vulnerability afflicted devices created by Animas, Bionet, and Roche. Susceptible Animas products included the AF24, a radio designed to communicate with the medical devices such as cardiac pacemakers, implantable neurostimulators, and implantable infusion pumps. Other critical issues impacted devices manufactured by Omron Corporation, primarily known for the distribution of medical devices, was the ProFTPD

Information Disclosure. This allows unauthorized users to access information transmitted by medical devices.

The second most common critical vulnerability was the MS17-010 security update. Like the Dropbear SSH Server issue, attackers can execute remote code on susceptible machines. Attackers that successfully exploit this vulnerability can run commands remotely on the local machine giving them complete access to the machine. Our results showed that this vulnerability was found in MRI scanners and X-Ray machines as well as devices produced by Carefusion and ReliOn. Lastly, we identified devices with Electronic Health Records (EHR) software that have SNMP default community names. Attackers can exploit these machines to gain a foothold into their respective networks and laterally move to other machines on the network.

Vulnerabilities in the high-risk threshold category pertain to servers running outdated versions of PHP with several known vulnerabilities. Common attacks against these vulnerabilities include Denial of Service (DoS) and remote code execution. Various infusion pumps contain these vulnerabilities. Similar to the MS17-010 vulnerability, this allows someone to perform actions on the system using its command line and potentially alter the dosage of medicine administered to patients. Lastly, the OpenSSH vulnerability impacting X-Ray machines, i-CAT scanners, blood pressure monitors, and FORA devices allows attackers to bypass authentication on a system and gain access to sensitive patient information with the device.

TABLE II. SELECTED NESSUS RESULTS

| Risk Category | Vulnerability | Number of Devices | Devices and Vendors | Products or Product Types |
|---|---|---|---|---|
| Critical | Dropbear SSH Server < 2016.72 Multiple Vulnerabilities | 104 | Animas, Bionet, Roche | AF24, R5N, AG5-HP, NB5 |
| | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (uncredentialed check) | 90 | Carefusion, ReliOn, MRI, X-Ray | Servers |
| | SNMP Agent Default Community Names | 64 | EHR | SNMP servers |
| High | PHP < 5.3.9 Multiple Vulnerabilities | 42 | Infusion | Microsoft IIS |
| | PHP < 4.4.5 Multiple Vulnerabilities | 23 | Infusion | Web servers |
| | OpenSSH MaxAuthTries Bypass | 22 | FORA, X-Ray, Blood Pressure, i-CAT | SSH servers |

## V. CONCLUSION AND FUTURE DIRECTIONS

Although the Internet has provided the medical field with many benefits, it has also raised major security concerns. This study aimed to discover vulnerabilities on networked medical devices identified from the Shodan database. Results of our preliminary study indicate that major vendor such as Animas, Bionet, Roche, and ReliOn are afflicted with Dropbear SSH server issues, PHP vulnerabilities, and OpenSSH weaknesses by allowing remote code execution and/or authentication bypassing.

There are several promising directions for future work. First, future studies can significantly expand the coverage of vulnerability assessment by analyzing all the medical devices on Shodan. Second, studies can aim to attribute who vulnerable devices belong to such that the owners are aware of their vulnerabilities. Finally, automatic mitigation strategies can be developed to patch and secure the detected vulnerabilities. All of the aforementioned directions would aid in developing critically needed medical device security capabilities.

## ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. NSF DUE-1303362 (SFS).

## REFERENCES

[1] Hiltzik, Michael. "Anthem Is Warning Consumers about Its Huge Data Breach. Here's a Translation." *Los Angeles Times*. Los Angeles Times, 6 Mar. 2015. Web. 14 Feb. 2017.

[2] Reuters. "Premera Blue Cross Says Data Breach Exposed Medical Data." *The New York Times*. The New York Times, 17 Mar. 2015. Web. 20 Feb. 2017.

[3] "Cyber Breach Hits 10 Million Excellus Healthcare Customers." *USA Today*. Gannett Satellite Information Network, 10 Sept. 2015. Web. 18 Feb. 2017.

[4] "Cybersecurity." *American Hospital Association*. 12 Sept. 2016. Web. 16 Feb. 2017.

[5] Peterson, Andrea. "Connected Medical Devices: The Internet of Things-that-could-kill-you."*The Washington Post*. WP Company, 03 Aug. 2015. Web. 23 Feb. 2017.

[6] Sayer, Peter. "Implantable Medical Devices Can Be Hacked to Harm Patients."*Computerworld*. IDG News Service, 01 Dec. 2016. Web. 23 Feb. 2017.

[7] Lake, David et al. “Internet of Things : Architectural Framework for eHealth Security.” 3 (2013): 301–328. Web.

[8] Sametinger, Johannes et al. “Security Challenges for Medical Devices.” 58.4 (2015): 1–8. Web.

[9] Halperin, Daniel et al. “Security and Privacy for Implantable Medical Devices.” (2008). pag. Print.

[10] FDA. “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and.” (2014): n. pag. Print.

[11] Kaplan, Dan. "Black Hat: Insulin Pumps Can Be Hacked." *SC Magazine US*. N.p., 10 Aug. 2011. Web. 11 Apr. 2017.

[12] Lybrand, Charles D. “The Use of Vulnerability Assessments : A Survey.” (2013). pag. Print.

[13] Samtani, Sagar et al. “Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques.” n. pag. Print.

[14] Patton, Mark et al. “Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT).” *Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014* (2014): 232–235. Web.

[15] Weidman, Georgia. Penetration Testing: A Hands-on Introduction to Hacking. N.p.: No Starch, 2014. Print.

[16] Mukhopadhyay, Indraneel, Shilpam Goswami, and Eshita Mandal. “Web Penetration Testing Using Nessus and Metasploit Tool Web Penetration Testing Using Nessus and Metasploit Tool.” March (2016): n. pag. We