4-24-2020

An Analysis on Medical Device Recalls and Cybersecurity Implications on Patient Safety

Rachel N. Leone
Boise State University

Liljana Babinkostova
Boise State University

Marion Scheepers
Boise State University

Kristen Garcia
Boise State University

Sulema Jimenez
Boise State University

See next page for additional authors

Authors

Rachel N. Leone, Liljana Babinkostova, Marion Scheepers, Kristen Garcia, Sulema Jimenez, and Tabarak Alomar

AN ANALYSIS OF MEDICAL DEVICE RECALLS

Kristen Garcia, Sulema Jimenez, Tabarak Alomar and Rachel Leone

BOISE STATE UNIVERSITY

NSF

Medical Device Cybersecurity Implications on Patient Safety

INTRODUCTION

According to the Food and Drug Administration (FDA) a recall is the removal or correction of medical devices that do not abide by the laws governed by the FDA and threaten patient health and safety [1]. Even though medical devices have become more advanced and are able to connect to networks and other devices, cybersecurity has become an issue while ensuring proper patient care. A recent study examined cybersecurity attacks in medical devices, then characterized the vulnerabilities based on reports from the CVE and ICS-CERT databases [3]. This analysis of FDA reports [2] are the preliminary actions to categorize medical device recalls and eventually connect them to potential cybersecurity vulnerabilities.

Retrieved from *Clear And Present Danger: Act Now On Medical Device Cybersecurity.*

METHODS AND DATA

Data was collected from the FDA Medical Device Recall Database from January 2010-March 2020 by entering “software” and “hardware” reasons into the search engine and yielded approximately 1300 results. The total number of software and hardware-related device recalls is shown by year in Figure 1.

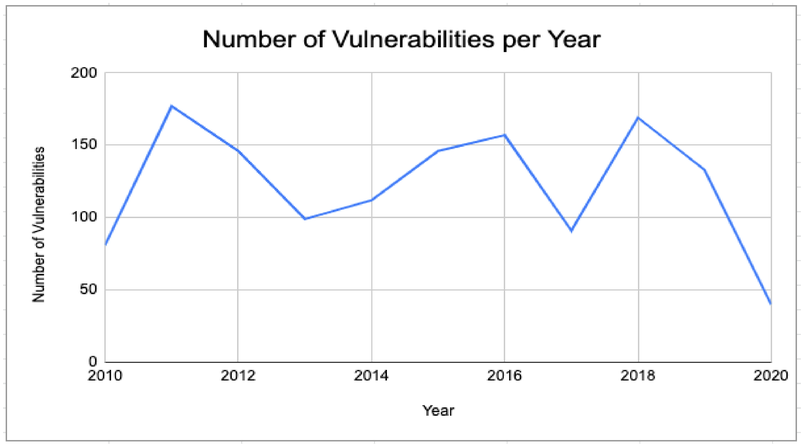

Figure 1: Number of Vulnerabilities Per Year Recorded in the FDA Database.

The R Suite and R Studio were used to assess all 1300 entries of data and sorted the dataset by number of recalled devices per manufacturer. The number of device recalls for the ten manufacturers with the greatest amount of software and hardware-related recalls are shown in Figure 2.

METHODS AND DATA

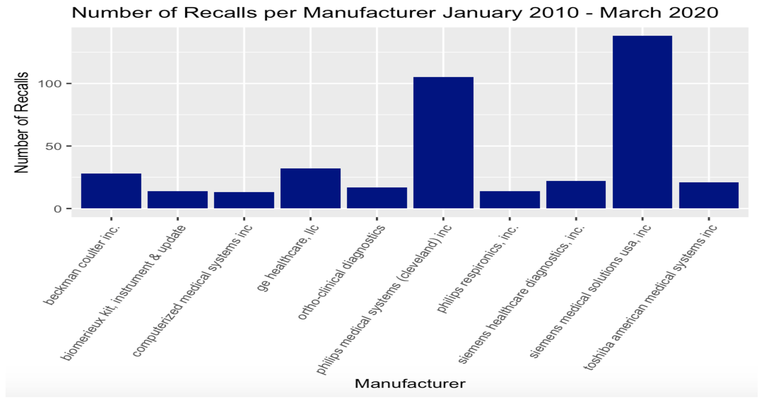

Figure 2: The ten manufacturers with the most device vulnerabilities between January 2010 - March 2020.

The entries from the top ten manufacturers were categorized by utilizing a keyword-based method the manufacturer’s reason for recall. Keywords were manually grouped together into categories, shown in Table 1. The proportions of these categories are shown in Figure 3.

Category	Keyword Samples
Multiple	**“multiple issues”, “numerous issues”**
Incorrect Data	**“incorrect values”, “error in”**
Loss of data	**“delayed diagnosis”, “exam to fail”**
Images and Results	**“rescans”, “same image”**
Patients	**“wrong patient”, “mistreatment”**
Damages	**“thermal damage”, “overheating”**
Software	**“upgrade”, “updated”**
System Processing	**“system crash”, “no access”**
Saving	**“not saved”, “collimation”**
Other	**“position sensor”, “mishandling”**

Table 1: Categorizations for Manufacturer Reason for Recall

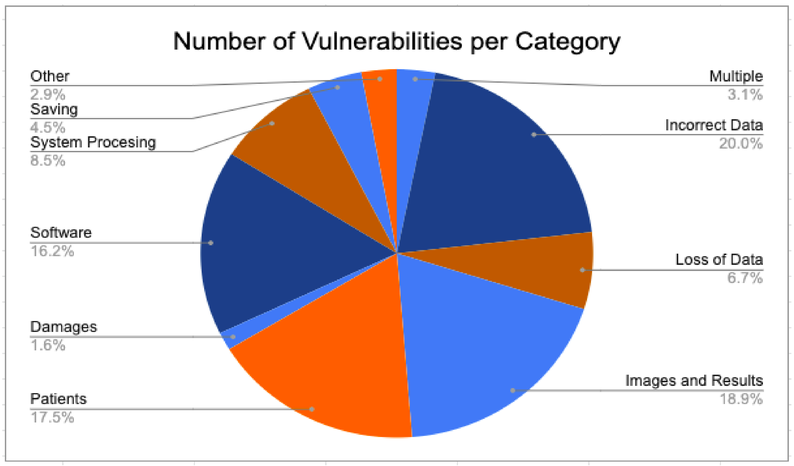

Figure 3: The number of vulnerabilities per category for the devices that were recalled by the top 10 highest manufacturers.

METHODS AND DATA

Phrases composing the previous categories were manually analyzed for possible cybersecurity-related issues in Figure 4.

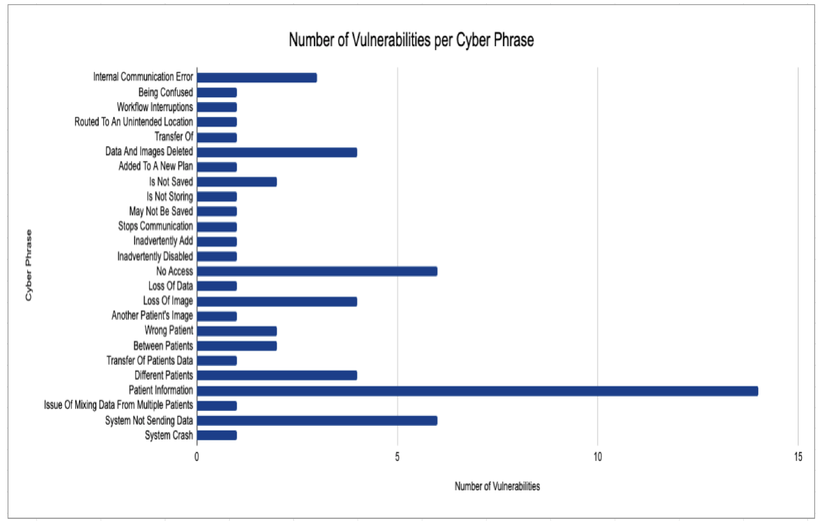

Figure 3: Number of Possible Vulnerabilities Per Cybersecurity-Related Manufacturer Reason for Recall Phrase.

CONCLUSION/FUTURE WORK

- Our preliminary results indicate that there are many types of medical devices and reasons for recall. The manufacturer’s reason for recall is more specific than the FDA’s reason, so patients may not understand the errors in their devices and the impact these errors can have on their safety and privacy due to the report. Therefore, using the manufacturer’s reason may provide more transparency for the patient.
- Develop a Natural Processing Language (NPL) software to categorize current and future recalls into a more manageable database for ease of patient access, while also linking these reasons for recall to the CVE and ICS-CERT classifications of software and cybersecurity malfunctions.

REFERENCES

[1] Center for Devices and Radiological Health, FDA. “Recalls, Corrections and Removals (Devices).” *U.S. Food and Drug Administration*, FDA,

[2] U.S. Food & Drug Administration. “Medical Device Recalls.” *Accessdata.fda.gov*,

[3] Y. Xu, D. Tran, Y. Tian and H. Alemzadeh, "Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices," *2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Arlington, VA, USA, 2019, pp. 23-24.

ACKNOWLEDGEMENTS

This research was supported by NSF REU Site Grant DMS-169872. We thank the Boise State College of Innovation and Design for their support of the project as well as our mentors Dr. L. Babinkostova, R. Erbes (Idaho National Lab), J. Radcliffe (Thermo Fisher Scientific), and Dr. M. Scheepers. We would also like to thank D. Leone, D. Valiente, and G. Frandsen for discussing our data analysis.