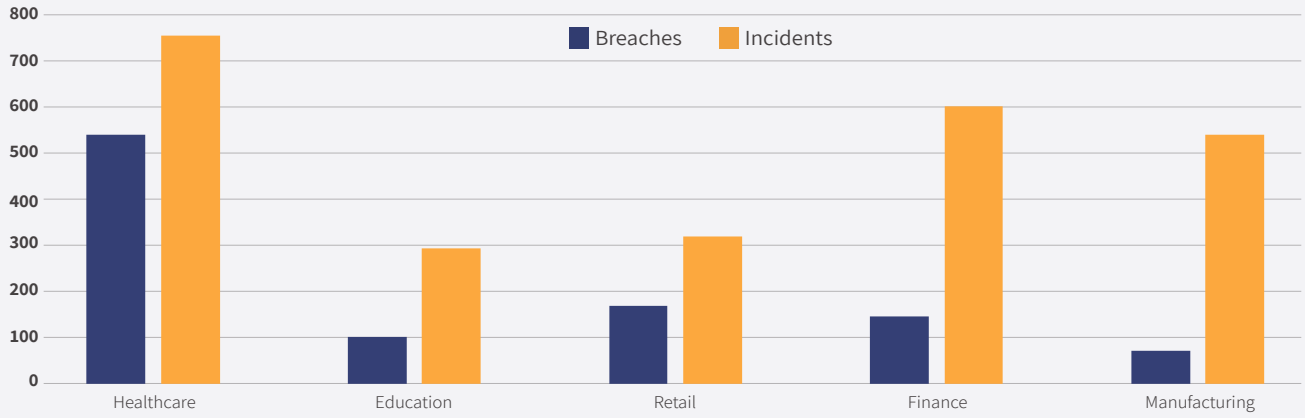
MEDIGATE

Manufacturer - Researcher Collaboration for Mitigating Vulnerabilities in Medical Devices

No technology product is guaranteed to remain 100% secure throughout its lifecycle. Once on the market, security researchers continually inspect products for vulnerabilities in their software and firmware, and manufacturers issue patches and security fixes to protect customers from falling victim to attackers. In spite of preliminary security reviews, vulnerabilities can go undetected throughout the pre-market security testing process, until its exploitation by cyber attackers. Technology and software products must undergo constant inspection by both security researchers and malicious actors as well as issue regular updates to keep their users' systems safe.

Data Breaches and Incidents by Sector, 2018[1]



Medical devices, however, do not always receive the same intensive security maintenance as technology products in other industries . While other industries have large communities of researchers looking for security weaknesses, finding a medical device weakness is almost completely dependent on manufacturers. First, getting access to medical devices is difficult. Not only are these products expensive, but one must own a license to purchase them. Furthermore, medical device manufacturers typically do not publish their products' firmware, taking the "security by obscurity" approach.

This approach relies on secrecy as a key security method. If no one can access the firmware, no one can hack it, right? Wrong. Not only is there no access to outside help, there is also no access to analysis from experts who could provide value to the vulnerability identification process. When cybercriminals manage to acquire the equipment or encounter it on an accessible network, finding a breach becomes relatively simple. Having security researchers digging into the code of medical devices, identifying vulnerabilities and publishing their findings independently or with the manufacturers, is crucial to the process of ensuring devices remain safe.

[1] Verizon Data Breach Investigation Report, 2018

Increase in Vulnerability Reporting

Vulnerability reporting is currently on the rise. During 2017, more than double the number of reports were documented in the National Vulnerabilities Database (NVD) over any other year. And already in the first half of 2018, more reports have been received than the entire year for 2015 and 2016[2]. Over the past few months researchers and manufacturers disclosed vulnerabilities in various medical devices, as published by the Industrial Control Systems Cyber Emergency Response Team (ICT-CERT). From CT scanners to implantable cardiac devices to medication and supply management products, there seems to be no resistant device type. In some cases, the vulnerabilities were identified by independent security researchers, while in others the manufacturers found them. This increased reporting of vulnerabilities is a positive trend for the security of medical devices, as all stakeholders will benefit from more researchers investigating medical devices, and more vulnerabilities amended. But this trend's success relies on efficient vulnerability disclosure processes, a highly debated topic these days.

Types of Vulnerability Disclosures

Vulnerability disclosures follow one of two models: full disclosure, in which the vulnerability is immediately published publicly, and coordinated vulnerability disclosure, in which the vulnerability is only disclosed after sufficient time has passed allowing for a patch or mitigation to be developed. In this process, security researchers that identify vulnerabilities first privately contact the manufacturer to give them an opportunity to fix the problem before they disclose the vulnerability to the public. Diagnosing and amending the issue usually requires continuous communication between the researchers who identified the vulnerability and the manufacturer. Coordinated work is also needed to solve the problem effectively while minimizing the time before notifying customers, as closing discovered vulnerabilities takes about 60 days on average today.

Coordinated Vulnerability Disclosure Best Practice

Philips and Medigate collaborated to disclose and mitigate three vulnerabilities potentially putting Philips IntelliVue Patient Monitors, and Avalon Fetal/Maternal Monitors at risk of improper authentication, information exposure and stack-based buffer overflow. Once Medigate identified and informed Philips of the vulnerabilities by way of Philips' coordinated vulnerability disclosure process, Philips quickly reviewed and verified them. They acted swiftly to resolve the vulnerabilities on the identified device and develop a patch with the assistance of Medigate to ensure a complete and thorough solution to the vulnerabilities for their customers.

Quick mitigation of vulnerabilities is extremely important, because the disclosure in itself increases the risk to users. An empirical study of zero-day attacks conducted by Symantec Research Labs found that after disclosing zero-day vulnerabilities, the volume of attacks exploiting them increases by up to 5 orders of magnitude[3]. Coordinated vulnerability disclosure aims to minimize the time between public disclosure and patching through researcher-manufacturer cooperation, leading to issuing a patch in close proximity to the disclosure.

[2] NVD Statistics retrieved from https://nvd.nist.gov/vuln/search
[3] Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World, Symantec Research Lab, 2012

The coordinated vulnerability disclosure model is not always as efficient or collaborative as it could be. Public pressure for full disclosure may be effective in forcing manufacturers to issue a timely solution for identified vulnerabilities; but, some manufacturers make it difficult for researchers to even report vulnerabilities by not maintaining communication channels and/or clear reporting policies. On the other hand, customer confidence increases when manufacturers and researchers work together, fix vulnerabilities and coordinate disclosures.

> **“Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure.”**
>
> Bruce Schneier
> Schneier on Security Blog

Summary

To provide the highest level of security for connected medical devices, tighter cross-industry cooperation is needed between manufacturing and medical devices security researchers. The recent spike in vulnerabilities reporting will hopefully mark the beginning of more collaborative work process. Everyone in the healthcare sector will benefit from medical devices whose security features are inspected more closely and by a greater community.

MEDIGATE

contact@medigate.io
www.medigate.io