HIMSS

transforming health through information and technology™

HIMSS
Healthcare and Cross-Sector Cybersecurity
Report

www.himss.org

HIMSS®

Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 24 – June 2018

Authored by: Lee Kim, BS, JD, CISSP, CIPP/US, FHIMSS
Director, Privacy and Security, HIMSS North America

Threat, Vulnerability, and Mitigation Information

1. ICS-CERT has issued Advisory (ICSMA-18-179-01) regarding the use of a hard-coded password and other vulnerabilities which, if exploited, may allow privileged access to the monitor's operating system. When the patient monitor is operated within close proximity of an implantable cardiac device, the exploitation of these vulnerabilities may allow an attacker to read and write arbitrary memory values to that device.

2. There have been some reports of a major Internet Service provider that had its web portal taken over and defaced by hackers. Yet others are reporting a massive outage with the Internet Service Provider as of June 29, 2018. Still others who are subscribers of another major Internet Service provider also reported problems.

3. Cybersecurity experts are predicting that application programming interfaces (APIs) will be exploited to hack enterprises. Common exploits include man in the middle attacks, session cookie tampering, and distributed denial of service attacks.

Reports and Tools

1. Stakeholders have developed an interactive tool which provides detailed data about supply and demand in the cybersecurity job market. Employers, educators and career counselors, and students may find information of interest using this tool.

2. Researchers have noted a significant trend in using Unicode "confusables" to register "fake" domain names with homographs. These domain names may be used to set up a phishing website by attackers to trick victims into visiting these sites.

3. Researchers have proposed the use of quantum key distribution to distribute unique keys between two users. Quantum key distribution may be combined with one-time pads to encrypt messages. However, this, according to researchers, requires extremely fast random number generators (namely, quantum random number generators). With the use of quantum random number generators, unpredictable cryptographic keys may be produced. The aim is to essentially provide a method for, essentially, unbreakable encryption.

4. Researchers have disclosed a way to exploit USB as a vector of attack, namely, by targeting hidden networks created with USB devices. Mitigation information is also disclosed. Additional information may be found here, here, and here.

5. The Centre for European Policy Studies (CEPS) has called upon the European Commission and its member states to draft a European-level framework with national legislation that provides legal clarity for software vulnerability discovery and disclosure. One of the recommendations is to have national computer emergency response teams (CERTs) to put into place frameworks for coordinated vulnerability disclosure that are similar to the ones adopted in the United States and Netherlands.

Special Announcements

1. Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders and healthcare constituents to discuss and learn about advancing the state of cybersecurity in the healthcare sector. All HIMSS members are welcome!