HIMSS

transforming health through information and technology™

HIMSS Healthcare and Cross-Sector Cybersecurity Report

Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 28 – November/December 2018

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

Threat, Vulnerability, and Mitigation Information

1. According to NIST, there is a vulnerability "[i]n all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection." This has been fixed in all supported Kubernetes releases.

   Proof of concept exploits are publicly available, including for authenticated and unauthenticated attacks. An additional explanation of this vulnerability may be found here and here.

2. According to this article, building industrial control systems are vulnerable to attack through cyber means, particularly through port 1911. The default port 1911 can serve up building information without the need to authenticate.

3. Beware of the phish – there has been an uptick recently in credential phishing, including those targeting popular web mail services. A white paper on combatting phishing may be found here.

4. This article describes methodology on how to remotely brick a server, explaining that present security defenses do not focus on firmware or hardware.

5. The worst passwords list has been published and "123456" is the most used password followed by "password" as the second most used password. This should be no surprise, including to people who maintain lists of common credentials.

6. According to researchers, cryptomining is beating out ransomware as a top cyber threat, including in the Middle East, Turkey, and Africa.

7. Two Christmas-themed DOS viruses have been released. The video may be found here.

Reports and Tools

1. A resource has been released to explain how Active Directory may be compromised and steps on how to mitigate, detect, and prevent.

2. A presentation on various red team tips can be found here.

3. A new vector for homograph attacks may be found here.

4. The MITRE Cyber Analytics Repository can be viewed using the CAR Exploration Tool here.

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!