May 8, 2018

TLP White

We start with a new vulnerability discovered in a multinational energy company's software and then address a Wi-Fi flaw associated with medical devices. We also discuss the impact voice assistant devices are having on doctors and shed some light on Artificial Intelligence in healthcare. We conclude with a discussion on Microsoft's new approach to IoT and ICS Devices. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Critically Flawed.*** Cybersecurity firm Tenable recently announced discovery of a critical-infrastructure software flaw impacting multinational energy company Schneider Electrics.[1] The flaw, if exploited, could allow potential hackers to shut down power plants, water systems and solar power facilities remotely. This revelation is particularly troublesome, coming just weeks after U.S. officials warned that Russian government hackers were targeting the U.S. energy and manufacturing sectors, among others, in a two-year, multi-stage intrusion campaign.[2]

   Despite the flaw's unsettling potential impact, the good news lies in how Schenider Electric responded to Tenable's discovery. The company was prompt in releasing the patch, and was proactive about sharing lessons learned with the cybersecurity community. This two-step approach of both addressing the problem and educating the larger community is not only commendable, but also an important component in the protection of all critical infrastructure sectors.

2. ***KRACK Bug.*** The KRACK vulnerability, short for Key Reinstallation attACKs, is an industrywide fundamental operation flaw in the Wi-Fi Protected Access II ("WPA2") protocol, which is intended to secure all modern protected Wi-Fi networks. In a recent advisory, ICS-CERT says that successful exploitation of the KRACK vulnerability "could allow data traffic manipulation, resulting in partial disclosure of encrypted communication or injection of data."[3] This particular advisory notes that the

1 https://www.tenable.com/blog/tenable-research-advisory-critical-schneider-electric-indusoft-web-studio-and-intouch-machine
2 https://www.us-cert.gov/ncas/alerts/TA18-074A
3 https://ics-cert.us-cert.gov/advisories/ICSMA-18-114-01

vulnerability has impacted versions of Becton, Dickson and Company ("BD") Pyxis, the company's medication and supply management system.

This vulnerability was originally discovered in October 2017[4], and as already mentioned, impacts nearly all WiFi enabled devices, not just medical devices, and certainly not only devices from BD. The fact that ICS-CERT only recently published this advisory is just part of their normal operations, and while concern over medical device security is something we all share, the focus some have taken on highlighting the risk has overshadowed some important facts and lessons worth your consideration.

According to a bulletin published by BD and referenced by ICS-CERT, KRACK can be exploited from an adjacent network with no privileges or user interaction required. However, the bulletin goes on to state that the attack complexity is high because the attack requires proximity to an affected Wi-Fi access point as well as significant technical expertise.[5]

The bulletin further explains that BD has implemented third-party vendor patches through BD's routine patch deployment process. As an additional remedial measure, BD provided the following recommendations to help reduce risk associated with the KRACK vulnerability:

- Ensure the latest recommended updates for Wi-Fi access points have been implemented in Wi-Fi enabled networks
- Ensure appropriate physical controls are in place to prevent attackers from being within physical range of an affected Wi-Fi access point and client
- Ensure data has been backed up and stored according to your organizational processes and disaster recovery procedures

Taking a step back, let's look at how BD responded to this:

- They acknowledged the vulnerability;
- They coordinated with ICS-CERT and other vendors;
- They quickly validated vendor patches to remediate the issue; and
- They provided detailed and accurate guidance for customers.

For those who are not familiar with the notion of Coordinated Vulnerability Disclosure ("CVD")[6], BD is a good example of how companies should respond when vulnerabilities are found in their products or services, and all companies should have similar policies

4 https://threatpost.com/krack-attack-devastates-wi-fi-security/128461/
5 https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletin-for-wpa2-krack-wi-fi-vulnerability
6 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

and procedures in place. Failure to do so can result in confusion, lengthier response times, and increased risk that organizational reputation can be damaged.

3. ***Tech News. Voice Assistants and Doctors.*** Doctors are beginning to use voice assistant devices to manage their administrative work and build stronger patient relationships because they argue that the transition from handwritten to electronic records has become a distraction.[7]

   The latest devices, "Suki" and "Sorpis" rely on artificial intelligence and natural language algorithms to record and organize the doctor/patient conversation into electronic health records ("EHR"). For example, the devices are equipped to respond to requests such as, "Prescribe Mark erythromycin and schedule him for a follow up appointment in 10 days."

   However, unlike conventional voice assistants like Alexa and Siri, both Suki and Sorpis are HIPAA-compliant. For example, both assistants (1) encrypt audio files at rest and in-transit to a HIPAA-compliant cloud; (2) utilize a listening prompt for activation; and (3) require patients to opt-in to being recorded.

4. ***Tech News. AI and Healthcare.*** A panel at the World Medical Innovation Forum discussed the costs and benefits associated with Artificial Intelligence ("AI"), which includes machine learning, natural language processing, cognitive computing, and speech and image recognition.[8]

   According to Stephen McHale, 23Bell Managing Partner, "AI can be on the defensive, and AI can go on the offensive…[and] [i]t is going to be an arms race." Jigar Kadakia, Partners Healthcare System Chief Information and Privacy Officer stressed a risk-based approach to AI use and Carl Kraenzel, IBM Watson Health Chief Information Security Officer, argued that AI can help organizations mitigate existing breaches. However, Kraenzel warned about the importance of paying attention to content curation to reduce the likelihood of creating unintended biases. Kraenzel also discussed IBM's new partnership with MIT to promote AI in healthcare.

   AI is promising but like many of the technologies we discuss, it comes with a risk. Members should always be cognizant of how they plan to utilize and rely on AI when conducting their business.

5. ***Tech News. Microsoft's Approach to IoT and ICS.*** Microsoft recently announced a new approach to secure Internet of Things ("IoT") and Industrial Control System ("ICS")

[7] https://www.wired.com/story/does-your-doctor-need-a-voice-assistant
[8] https://healthitsecurity.com/news/ai-can-bolster-or-undermine-healthcare-data-security-panel-says

Devices.[9] The project, deemed "Trusted Cyber Physical Systems," ("TCPS") uses three components to identify and block intrusions and its goal is to secure data-in-execution in addition to data-at-rest and in-transit.

The first component, focusing on hardware, relies on Trusted Execution Environments ("TEE") such as the Intel SGX, ARM TrustZone, and SecureElements, to separate areas of the CPU that process highly-sensitive data from the rest of the CPU. The second component is a graphical user interface (GUI) that, according to Microsoft, acts as a "Secured Confirmation Terminal" and is controlled by a designated employee. The designated employee, through the GUI is able to detect and block malware that attempts to enter into the IoT/ICS systems. The third component utilizes a cloud-based platform capable of (1) provisioning, (2) key and patch management, (3) certificate authority, and (4) secure logging.

These advancements are crucial to ensuring that IoT and ICS are as secure as possible, particularly given the proliferation of these devices. Nevertheless, every organization's risk is their own, and as we've talked about before, a good risk management program will incorporate IoT and ICS wherever they are used.

Congress –

Tuesday, May 8:
--No relevant hearings

Wednesday, May 9:
--No relevant hearings

Thursday, May 10:
--No relevant hearings

Conferences and Webinars –

<https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--Medical Device and Pharmaceutical Security Workshop – London
<https://nhisac.org/events/nhisac-events/security-workshops-london/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17)
<http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>

[9] https://www.bleepingcomputer.com/news/security/microsoft-wants-to-secure-iot-and-ics-devices-with-new-tcps-project/

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21)
<https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29)
<https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Is it Time to Regulate Cyber Conflicts?**
<https://www.lawfareblog.com/it-time-regulate-cyber-conflicts>
-- **Kaspersky Details New ZooPark APT Targeting Android Users**
< https://www.bleepingcomputer.com/news/security/kaspersky-details-new-zoopark-apt-targeting-android-users/>
-- **Nigerian Email Scammers Are More Effective Than Ever**
<https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever>
--**Report: China's Intelligence Apparatus Linked to Previously Unconnected Threat Groups**
< https://www.darkreading.com/attacks-breaches/report-chinas-intelligence-apparatus-linked-to-previously-unconnected-threat-groups/d/d-id/1331724>
--**Facebook to play cupid in online dating debut**
<http://feeds.reuters.com/~r/reuters/topNews/~3/bcuDfadMQ6o/facebook-to-play-cupid-in-online-dating-debut-idUSKBN1I23YV>
-- **Foreign companies increasingly focus of government leaders' cyber, surveillance fears**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/05/04/foreign-companies-increasingly-focus-of-government-leaders-cyber-surveillance-fears-204664>
-- **Consumer anger over Equifax, but Washington stands still**
< https://www.politico.com/newsletters/morning-cybersecurity/2018/05/01/consumer-anger-over-equifax-but-washington-stands-still-198871>
-- **Twitter warns all users to change passwords after discovering internal bug**
<https://www.cyberscoop.com/twitter-password-bug/>
-- **Pentagon bars Huawei, ZTE devices from sale on military bases**
< https://www.cyberscoop.com/huawei-zte-pentagon-ban-military-bases/>

May 8, 2018

-- **Pennsylvania experts review election cybersecurity**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/05/03/pennsylvania-experts-review-election-cybersecurity-202733>

Contact us: follow @NHISAC and email at newsletter@nhisac.org