October 30, 2018

TLP White

This week we start a deeper dive into Coordinated Vulnerability Disclosure ("CVD"). We start with what CVD is and its origins, with a focus on the relationship between manufacturers of software and hardware with vulnerability researchers. We take a brief look at significant vulnerabilities from the last few years that have elevated the CVD discussion, as well as specific CVD applications in the health care sector. We conclude with some things to consider with respect to your organization's approach to vulnerability disclosure.

Welcome back to *Hacking Healthcare:*

Coordinated Vulnerability Disclosure: What Is It?

No organization can manage the complex and interconnected technology systems on which they depend on their own. Despite continuing advancements in the development of secure hardware and software, identification and mitigation of vulnerabilities continues to be one of greatest challenges facing organizations across all sectors.

Over the years, this has led to a robust ecosystem of researchers, companies, standards, policies, and technologies designed to identify vulnerabilities in every piece of hardware, software and service connected to the Internet. This in turn led to the need for a standardized and predictable way for researchers to reach out to organizations who may be either the creator/maintainer of the software, product or service, or who may fall victim to it. This multi-stakeholder process is known as coordinated vulnerability disclosure.

At the simplest level, coordinated vulnerability disclosure is the process by which researchers who find vulnerabilities communicate with the organization that owns the service, product or software where the vulnerability was discovered. For example, if a researcher found that a company website had a vulnerability that would allow a hacker to intercept credit card information, they would want to report it to that company so that the vulnerability could be addressed. Or they may discover an exploitable vulnerability in a medical device that could lead to patient harm. Researchers have varying reasons for doing this, but there is a standardized process that they expect organizations to follow, as discussed below. This same process also tells the researcher what the organizations expects of them, which is equally, if not more important.

October 30, 2018

CVD Use Cases: Heartbleed, Meltdown/Spectre

To understand the importance of CVD, it is helpful to think about recent, large scale vulnerabilities and their impact. Heartbleed is one example of a vulnerability that impacted many major websites, including Tumblr, Google, Yahoo, Dropbox, Netflix, and more.[1] Heartbleed is a vulnerability in certain versions of OpenSSL, an open-source cryptographic library and could allow attackers to bypass secure servers and access encrypted information without detection. Major Websites like Google and Tumblr had the resources available to quickly fix the flaw. However, smaller organizations had a more difficult time remediating Heartbleed, in some cases due to legacy systems that were difficult or costly to upgrade, and in other cases because they were less likely to know that their device was running OpenSSL, let alone how to remediate the flaw.

Meltdown and Spectre are another example of widespread, multiparty vulnerabilities that has impacted a significant number of devices. Meltdown and Spectre are related to a hardware vulnerability in central processing units that permit access to an operating system's memory. Through this unauthorized access, an attacker can exploit the vulnerabilities to expose sensitive data, including passwords, cryptographic keys, personal photos, emails or any other data stored on impacted personal computers, mobile devices, and in the cloud.

In the above use cases, among others, it was critical for researchers and organizations to collaborate in order to develop and issue a fix, and to make sure that the right people knew about it at the right time so that the vulnerability was not turned into a means of attack. With vulnerabilities this big, fumbling that process could have serious consequences.

CVD Best Practices for Healthcare Organizations

CVD programs had informal beginnings, but have increasingly been acknowledged by regulators and industry leaders as an important component of an organization's cybersecurity practices. The House Energy and Commerce Committee recently published a white paper containing recommendations to support public and private sector organizations in their adoption of CVD programs as part of their cybersecurity risk management strategies.[2] The Food and Drug Administration ("FDA"), as part of its growing emphasis on medical device security, recommends that companies have a structured and systematic approach to risk management.[3] The FDA has also announced increased coordination between the agency and the Department of Homeland security, most notably to ensure shared responsibility for coordinated vulnerability disclosure for identifying and addressing cybersecurity risks.[4]

---

[1] https://www.vox.com/cards/heartbleed/have-there-been-any-successful-attacks-using-the-heartbleed-bug

[2] https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

[3]https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf?utm_campaign=FDA%20Releases%20Draft%20Recom%20on%20Premrkt%20Sub%20Manag%20Cybersecurity&utm_medium=email&utm_source=Eloqua

[4] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm623574.htm

Medical device trade association, the Advanced Medical Technology Association ("AdvaMed"), incorporated CVD in its 2017 AdvaMed Medical Device Cybersecurity Foundational Principles ("principles").[5] The principles provide that medical device manufacturers should support a coordinated disclosure process that provides a pathway for researchers and other third-parties to submit information to the company, including detected potential vulnerabilities.[6]

What We Have Learned and What You Should Be Doing

In the wake of major vulnerabilities such as Heartbleed, Spectre/Meltdown, and others, having a CVD program in place has evolved into a mission necessity. A CVD policy which outlines how a company will respond to a researcher's report that a product or service contains a vulnerability, signals to the researcher that the organization has already thought the process through and provides directions on how to get vulnerability information to the right person within an organization. After facing backlash from disgruntled companies following the discovery of a vulnerability, many researchers will not even notify a company about a known vulnerability if the company does not have a CVD policy in place.

Ultimately, the structure of the internet, and the growing number of connected devices, makes it nearly impossible for all companies to discover and fix vulnerabilities on their own without any help. Third-parties including researchers help the entire ecosystem by discovering vulnerabilities and sharing this critical information with organizations which may otherwise have missed it, or at least taken a long time to catch. With some forethought in establishing a CVD policy and program, organizations can be transparent about their CVD practices, and researchers can find some assurance that their discovery is not used against them. This collaborative approach, while not perfect, is the best way to keep systems safe without placing all of the burden on individual organizations.

Finally, recognize that CVD can be a complex and nuanced process that if not done correctly, may create more problems than it solves. Don't be afraid to ask for help in getting your own CVD program off the ground.

Congress –

<u>Tuesday, October 30</u>:
--No relevant hearings.

<u>Wednesday, October 31</u>:
--No relevant hearings.

---

[5]https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf

[6]https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf

Thursday, November 1:
--No relevant hearings.

International Hearings/Meetings –

EU –

Tuesday, November 13:
--Hearing entitled, "Assessing the impact of digital transformation of health services" (EU Commission's Expert Panel on Health).[7]

Conferences, Webinars, and Summits –

--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>
--Medical Device Security 101 Conference – Orlando, FL (1/21/19-1/22/19)
<https://nhisac.org/events/nhisac-events/medical-device-security-101-conference/>
--FIRST Symposium 2019 – London, UK (3/18/19)
<https://nhisac.org/events/nhisac-events/first-symposium-2019/>
--2019 NH-ISAC Spring Summit – Ponte Vedra Beach, FL (5/13/19-5/17/19)
<https://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

Sundries –

--**US federal privacy law? Apple, Google, Facebook, Microsoft all hope so**
<https://iapp.org/news/a/us-federal-privacy-law-apple-google-facebook-microsoft-all-hope-so/>
--**Retail Fraud Spikes Ahead of the Holidays**
<https://www.darkreading.com/vulnerabilities---threats/retail-fraud-spikes-ahead-of-the-holidays/d/d-id/1333130?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>
--**Two hackers behind 2016 Uber data breach have been indicted for another hack**
<https://techcrunch.com/2018/10/25/uber-hackers-indicted-lynda-breach/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29>
-- **UK watchdog hands Facebook maximum $500K fine over Cambridge Analytica data breach**

[7] https://ec.europa.eu/health/expert_panel/events_en

October 30, 2018

<https://techcrunch.com/2018/10/25/uk-watchdog-hands-facebook-500k-fine/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29>
--**British Airways has some good news and bad news about its payment breach**
<https://www.cyberscoop.com/british-airways-additional-customers-identified-magecart-breach/>
-- **Side-Channel Attack Exposes User Accounts on Facebook, XBox, Other Social Sites**
<https://www.darkreading.com/cloud/side-channel-attack-exposes-user-accounts-on-facebook-xbox-other-social-sites/d/d-id/1333125?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>

Contact us: follow @HealthISAC, and email at contact@h-isac.org