July 1st, 2020

TLP White

This week, Hacking Healthcare takes an in-depth look at one of the more unique and interesting governmental processes that has a significant influence on cybersecurity in the private sector. The Vulnerabilities Equities Process (VEP) may not be something you are familiar with, but it is important that healthcare sector entities are aware of what it is (and isn't), its impact, and what they can and should be doing in response to it. Welcome back to *Hacking Healthcare*.

1. Introduction

Hardware and software vulnerabilities, the flaws and bugs that exist in coding or physical architectures, are an unavoidable characteristic of modern technologies. These vulnerabilities can provide interested parties the opportunity to force a piece of software or hardware to perform unanticipated actions that produce results that are often at odds with the intention of the designer. When these vulnerabilities are used by malicious actors for ill intent, especially in critical infrastructure settings like the healthcare sector, the results can be disastrous.

This is even more true of zero-day vulnerabilities. These vulnerabilities are useful, monetarily valuable, and highly sought after because they are not widely known until their use. Therefore, they are unpatched, unmitigated, and open to potential exploitation.

Fortunately, not all individuals and organizations looking for these vulnerabilities are malicious. Many security researchers and other well-intentioned individuals would much rather see these previously unknown flaws fixed than watch them become exploited. Additionally, there is a growing acknowledgement among software and hardware developers that they should provide a means for such vulnerabilities to be securely reported to those in a position to fix them. While this is becoming a widespread industry best practice, it gets a bit more complicated where the public sector is concerned.

Governments and their various civil and military sub-entities are tasked with defending their citizens and organizations while simultaneously developing the capabilities to undermine adversaries. In effect, they must balance what are often competing offensive and defensive goals when it comes to determining how to handle zero-day vulnerabilities.

Intelligence agencies use software and hardware zero-day vulnerabilities to conduct espionage and intelligence gathering operations, and law enforcement officials can use them to gather evidence against criminals. Furthermore, the military may utilize vulnerabilities as offensive opportunities to degrade adversarial capabilities as part of a larger combined arms approach to warfare.

Defensively, agencies such as the United States' Cybersecurity and Infrastructure security Agency (CISA), which sits within the Department of Homeland Security (DHS), view these vulnerabilities as major threats to the functioning of critical infrastructure, the government, and society in general. In their view, zero-day vulnerabilities should be made known to the appropriate entities and subsequently patched as quickly as possible to avoid harm.

Within the United States' government, how these competing missions are ultimately reconciled is through something called the Vulnerabilities Equities Process (VEP). This week, we want to outline how this process works, how it affects the private sector, and what the healthcare industry can and should be doing in response.

The Vulnerability Equities Process (VEP)

What is it?

At a high-level, the VEP is the means by which various U.S. federal government stakeholders meet to coordinate how to handle discovered zero-day vulnerabilities. This process essentially determines if a zero-day vulnerability should be disclosed (to the vendor or developer) to be patched or retained for national security purposes.

Who developed it and when?

From the documents that have been publicly released, the initial concept of creating a VEP process came in 2008 as a product of President George W. Bush's administration.[1] Subsequently, the Office of the Director of National Intelligence (ODNI) led a working group that produced a VEP document in 2010, which was then updated after the Snowden NSA revelations to lean more clearly in favor of disclosing vulnerabilities to companies. Finally, it was updated again in 2017 by the White House's publication of the mostly unclassified charter, *Vulnerabilities Equities Policy and Process for the United States Government*.[2] This document modified the original process and provided much greater transparency surrounding the VEP process that is still in use today.[3]

Who participates and where does it sit?

In order to ensure that "competing considerations for disclosing or restricting a vulnerability" are fairly weighed, the VEP is not led by a single agency. Instead, the National Security Council (NSC) coordinates to ensure relevant stakeholders are able to provide adequate input.[4] Within the VEP sits two entities. First, there is the Equities Review Board (ERB), which acts as the "primary forum for interagency deliberation and determinations concerning the VEP."[5] Second, there is the National Security Agency (NSA) serviced VEP Executive Secretariat, which "[facilitates] information flow, discussions, determinations, documentation, and recordkeeping for the process." [6]

The ERB includes representation from the Office of Management and Budget (OMB), the Office of the Director of National Intelligence (ODNI), the Department of the Treasury (USDT), the Department of State (DOS), the Department of Justice (DOJ), the Department of Homeland Security (DHS), the Department of Energy (DOE), the Department of Defense (DOD), the Department of Commerce (DOC), and the Central Intelligence Agency (CIA). Other agencies may participate depending on circumstances. Notably, there is no private sector representation.

How does it work?

The process itself involves the following procedures:

1. *Submission*: When an agency is made aware of a zero-day vulnerability that meets the threshold for inclusion in the VEP process, it notifies the VEP Executive Secretariat and includes a recommendation of what should be done.
2. *Notification*: The VEP Executive Secretariat notifies the other governmental stakeholders and requests a response if they feel they have equity in the vulnerability that is being discussed.
3. *Equity and Discussion*: The governmental stakeholders that respond must state whether they agree or disagree with the initial notifying agency's recommendation. The VEP is designed to work towards complete consensus, and any disagreements are followed by discussions between the involved stakeholders to reach an agreement. If an agreement isn't reached, those involved offer up options to the ERB.
4. *Determination*: Ultimately, a determination on what to do with a vulnerability is to be made quickly; is to ensure that all the stakeholders have been part of the process; and is to be made "in the overall best interest of USG missions of cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection."[7]
5. *Contestation*: When a consensus cannot be reached, the ERB holds a vote. Those stakeholders contesting the outcome of that vote may appeal through an NSC process.
6. *Handling and Follow-on Actions*: If the consensus is that the vulnerability should be released, the disclosure is often led by the agency or department that initially submitted it, with all other stakeholders following agreed-upon disclosure guidelines. Additionally, the agency or department that discloses the vulnerability to the vendor must follow up with the vendor to ensure that appropriate measures were taken to address it. If the vendor decides not to address the vulnerability, or is not acting swiftly enough, the department or agency who disclosed it must notify the VEP Executive Secretariat and the government may take other actions to mitigate the vulnerability.

   If the consensus is that the vulnerability should be retained and information of its existence restricted, the vulnerability is then kept and annually reassessed through this process until it is released.

Just six easy steps! Of course, you don't have to look very hard to realize that things can get complicated in a hurry.

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, June 30th:
- No relevant meetings
Wednesday, July 1st:
- House – Committee on Armed Services: *Markup of H.R. 6395 - National Defense Authorization Act for Fiscal Year 2021*
Thursday, July 2nd:
- House – Committee on Small Business - Subcommittee on Economic Growth, Tax, and Capital Access: *Supply Chain Resiliency*
- Senate – Committee on Appropriations - Subcommittee on Departments of Labor, Health and Human Services, and Education, and Related Agencies: *Hearings to examine Operation Warp Speed, focusing on researching, manufacturing, and distributing a safe and effective coronavirus vaccine.*

International Hearings/Meetings –

EU – No relevant hearings

Conferences, Webinars, and Summits –

--How Authentication Attacks Threaten your Healthcare Environment by Qomplx – Webinar (7/1/2020)
https://h-isac.org/hisacevents/authentication-attacks-qomplx/
-- Enabling Interoperable Identity Across Healthcare with SAFE Identity – Webinar (7/9/2020)
--COVID-19 and its Cybersecurity Challenge – Webinar (7/9/2020)
https://h-isac.org/hisacevents/covid-19-and-its-cybersecurity-challenge/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Virtual (7/16/2020)
https://endeavor.swoogo.com/summer_virtual_healthcare_innovation_cybersecurity_forum/About
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
-- H-ISAC Monthly Member Threat Briefing – Webinar (7/28/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-10/
--H-ISAC Virtual Security Workshop – Virtual (7/29/2020)
https://h-isac.org/hisacevents/nz-virtual-workshop/
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020) - CANCELLED
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)

https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Forchheim, Germany (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

Sundries –

--California university pays $1 million ransom amid coronavirus research
https://www.cyberscoop.com/ucsf-ransomware-payment-coronavirus/
--Two record DDoSes disclosed this week underscore their growing menace
https://arstechnica.com/information-technology/2020/06/two-record-ddoses-disclosed-this-week-underscore-their-growing-menace/
-- After initial spike, telehealth visits are on the decline, report finds
https://www.healthcareitnews.com/news/after-initial-spike-telehealth-visits-are-decline-report-finds

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

[1] https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf
[2] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
[3] https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf
[4] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
[5] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
[6] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
[7] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF