Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 2eec682a | Mar 08, 2023, 12:51 PM

This week, Hacking Healthcare takes a longer look at coordinated vulnerability disclosure. We break down a new vulnerability disclosure legal framework that has been introduced by Belgium, analyze its benefits and potential shortcomings, and then end with a few recommendations for how all this applies to the healthcare sector.

Welcome back to *Hacking Healthcare*.

What Does Belgium's New Vulnerability Disclosure Framework Mean?

Last month, The Center for Cyber Security Belgium (CCB) announced a new legal framework for IT vulnerability reporting. The new framework sets out rules meant to provide security researchers and ethical hackers some legal safe harbor to "investigate and report existing vulnerabilities in networks and information systems located in Belgium".[1] Vulnerability disclosure can be a complicated topic for organizations, and while we have covered this issue in the past, Belgium's recently implemented vulnerability disclosure policy provides a good reason to revisit it.

Terminology

Before exploring Belgium's new policy and its broader implications, let's brush up on some key terms associated with vulnerability disclosure that are sometimes conflated.

- Vulnerability Disclosure Policy (VDP): VDP is a policy that describes how an organization would like outside entities to report cybersecurity vulnerabilities to them in order to be considered "good faith" efforts that won't result in legal action. VDPs often outline the scope of allowed activities, the manner in which vulnerabilities should be disclosed, the format and content of those disclosures, and what vulnerability reporters should expect in terms of follow-on engagement and vulnerability remediation.

- Coordinated Vulnerability Disclosure (CVD): As CERT/CC succinctly describes, a CVD "is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders and the public."[2]

- Bug Bounty: a monetary reward given to ethical hackers or security researchers for discovering and reporting a vulnerability to an organization. Bug bounties exist as a subset of VDPs, as rewards can be implemented into VDPs but are not a necessary component. Bug bounty programs also exist as a complement to, or replacement for, a VDP.

Belgium's New Policy

Belgium's CCB acknowledges that there are individuals that actively look for vulnerabilities with the laudable intent of reporting them so that cybersecurity can be improved.[3] However, they also note that this can happen without prior warning to, or permission from, the entity being examined. Without clear guidance or a trusted coordinator, navigating these kinds of interactions to a mutually beneficial end is typically fraught with legal grey areas.

In an effort to clarify how vulnerability reporting should work in Belgium, the CCB presented a new legal framework on February 15th. At a high level, this new framework sets out the expectations and requirements for security researchers and ethical hackers if they want safe harbor from various Belgian legal offenses that could conceivably be brought against their actions.

Here are some of the highlights:[4]

- If an organization has a VDP, and an individual finds a vulnerability within the scope of the VDP, the individual should report that vulnerability only to the organization
- If the organization fails to respond in a reasonable timeframe or other "difficulties arise," either party can contact the CCB to act as a lead coordinator
- If the vulnerability affects other organizations that do not have a VDP, the vulnerability can be reported to the CCB
- The CCB outlines obligations that include limiting actions to only what is "necessary and proportionate to verify the existence of a vulnerability"
- Individuals "may not attempt to monetize the information discovered" unless "a reward or remuneration has been explicitly and previously agreed upon"
- The CCB encourages security researchers to make themselves known to an organization before carrying out activities
- Individuals cannot "publicly disclose information about the discovered vulnerability without the agreement of the CCB"

Action & Analysis
Included With Health-ISAC Membership*

Congress
Tuesday, March 7th:
- No relevant hearings

Wednesday, March 8th:
- Senate – Committee on Security and Governmental Affairs: Hearings to examine artificial intelligence, focusing on risks and opportunities.

- House of Representatives – Committee on Oversight and Accountability: Hearing “Advances in AI: Are We Ready For a Tech Revolution?”

Thursday, March 9th:
- No relevant hearings

[1] https://ccb.belgium.be/en/vulnerability-reporting-ccb
[2] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330
[3] https://ccb.belgium.be/en/news/new-legal-framework-reporting-it-vulnerabilities
[4] https://ccb.belgium.be/en/vulnerability-reporting-ccb
[5] https://blog.intigriti.com/2023/01/19/new-belgian-legal-framework-gives-safe-harbor-to-ethical-hackers-and-bug-bounty-hunters/
[6] https://blog.intigriti.com/2023/01/19/new-belgian-legal-framework-gives-safe-harbor-to-ethical-hackers-and-bug-bounty-hunters/
[7] https://www.hackerone.com/ethical-hacker/what-does-belgiums-new-legal-framework-hacking-mean-me
[8] https://therecord.media/belgium-institutes-nationwide-vulnerability-disclosure-policy/
[9] https://therecord.media/cfaa-change-doj-good-faith-cybersecurity-research/
[10] https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu
[11] https://ccb.belgium.be/en/vulnerability-reporting-ccb
[12] https://ccb.belgium.be/en/vulnerability-reporting-ccb
[13] https://www.cisa.gov/vulnerability-disclosure-policy-template
[14] https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit
[15] https://ccb.belgium.be/en/coordinated-vulnerability-disclosure-policy-and-vulnerability-detection-reward-program-bug-bounty
[16] https://www.hackerone.com/ethical-hacker/what-does-belgiums-new-legal-framework-hacking-mean-me

---

Reference | References

The Record
Europa Analytics
intigriti
NCSC
Health-ISAC DDoS Whitepaper
Hackerone
belgium
The Record
belgium
cmu
belgium
CISA

Report Source(s)

Health-ISAC

Tags

Legislation, Hacking Healthcare, Vulnerability Disclosures , EU, Vulnerability Disclosure Policies, European Union (EU), Vulnerability Disclosure Policy, vulnerability disclosure, European Union

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.