hackerone

December 16, 2024

VIA ELECTRONIC SUBMISSION

Re: Request for Comment on Product Security Bad Practices Guidance - Docket No. CISA-2024-0028

Dear Sir or Madam:

HackerOne Inc. (HackerOne) submits the following comments in response to the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigations (FBI)'s request for feedback on the Product Security Bad Practices Guidance.[1] HackerOne appreciates the opportunity to provide input on this important matter, and we offer the following points for your consideration:

A Vulnerability Disclosure Policy (VDP) Is Best Practice for All Sectors

HackerOne agrees that the lack of a formal Vulnerability Disclosure Policy (VDP) constitutes a critical cybersecurity gap and a significant bad practice that should be addressed. We recommend that all organizations adopt clear and comprehensive VDPs to guide the reporting of security vulnerabilities.

While the current Bad Practices Guidance primarily focuses on critical infrastructure, HackerOne encourages CISA and the FBI to consider expanding the recommendation for implementing a formal VDP to include all systems, not just those classified as critical infrastructure. Cybersecurity is a fundamental concern for all organizations, and the adoption of VDPs can offer significant benefits to entities of all sizes. By promoting VDPs across all sectors, as emphasized in the National Cybersecurity Strategy, CISA can help foster a more inclusive and comprehensive cybersecurity posture that enhances the protection of the broader digital ecosystem.[2]

Why VDPs Are Beneficial

VDPs offer a structured and effective framework for receiving, identifying, and triaging vulnerability reports. Often referred to as the internet's "see something, say something" policy, VDPs encourage individuals to report security risks they encounter, allowing organizations to address these issues promptly before they can be exploited.[3] This proactive approach helps prevent data breaches, minimize security threats, and reduce the overall impact of vulnerabilities.

[1] Request for Comment on Product Security Bad Practices Guidance, Cybersecurity and Infrastructure Security Agency, 89 Fed. Reg. 83508, October 16, 2024. See also CISA, Product Security Bad Practices Guidance, Oct. 16, 2024, https://www.cisa.gov/resources-tools/resources/product-security-bad-practices.
[2] White House, National Cybersecurity Strategy, Mar. 2023, pg. 21, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[3] HackerOne VDP Report, https://www.hackerone.com/sites/default/files/2021-03/vulnerability-disclosure-policy-what-is-it-why-you-need-one-how-to-get-started.pdf

A robust VDP fosters trust between an organization and its key stakeholders—whether customers, citizens, or investors. It demonstrates a strong commitment to upholding cybersecurity best practices and protecting sensitive data.

Why the Lack of VDPs Is Detrimental

Without a VDP in place, organizations risk mishandling vulnerabilities, which can lead to delayed mitigation or, in the worst-case scenario, exploitation by malicious actors. Moreover, the lack of a VDP can severely damage trust between organizations and their key stakeholders. It signals a lack of commitment to cybersecurity, undermining confidence in the organization's ability to safeguard sensitive information. This erosion of trust can potentially lead to negative consequences, including reputational damage, legal repercussions, and financial losses.

Scope of Vulnerability Disclosure Policies (VDPs)

HackerOne encourages CISA and the FBI to incorporate additional critical VDP elements in the Bad Practices Guidance, drawing on best practices, standards, and other guidance such as the Department of Homeland Security's (DHS) Binding Operational Directive BOD 20-01:

1. **Systems in Scope:** Clearly define which systems or products are covered by the VDP, ensuring that security researchers know which assets are in scope for testing and which are off-limits.

2. **Types of Authorized Testing:** Specify the types of security testing that is allowed and outline the actions that are prohibited.

3. **Vulnerability Report Submission Process:** Provide a well-defined process for submitting vulnerability reports, including clear guidelines on what information is required. This should encompass:

    - **Disclosure Channels:** Designate easily accessible channels for submitting reports
    - **Required Information:** Outline what information is necessary for effective vulnerability analysis, such as descriptions of the vulnerability, its location, impact, technical details for reproduction and proof of concept.
    - **Anonymous Reporting:** Allow anonymous submissions to encourage participation from a broader range of security researchers.

4. **Safe Harbor:** Offer assurances that security researchers will not face legal consequences when submitting vulnerabilities in good faith.

5. **Acknowledgement and Transparency:** Clearly outline the expectations for acknowledging and responding to vulnerability reports, including:
    - **Timely Acknowledgement:** Commitment to acknowledge receipt of reports within a specified timeframe.

- **Transparency in Remediation:** Clear communication on how vulnerabilities will be addressed, including response times based on severity, timelines for public disclosure, and whether finders can expect confirmation.[4]

The absence of these critical elements would weaken the effectiveness of a VDP and constitute a bad practice. We urge CISA to integrate these recommendations into the final guidance on vulnerability disclosure.

* * *

HackerOne appreciates the work CISA and the FBI are doing to recognize the importance of VDPs as a foundational element of product security. Thank you for considering our comments. We look forward to the continued development of policies that will strengthen the cybersecurity posture of both the public and private sectors.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne

[4] https://docs.hackerone.com/en/articles/8368965-vdp-vs-bbp