Poster: A Glimpse of Vulnerability Disclosure Behaviors and Practices Using GitHub Projects

Jessy Ayala, Yu-Jye Tung, Joshua Garcia
Donald Bren School of Information and Computer Sciences
University of California, Irvine, USA

***Abstract*—In open-source software (OSS), the number of published software vulnerabilities has tremendously increased. The GitHub Advisory Database contains advisories for security risks in GitHub-hosted OSS projects. As of 04/14/2024, there are 213,594 unreviewed security advisories in GitHub Advisory Database. Of those unreviewed, at least 63,852 are publicly documented vulnerabilities, potentially leaving many OSS projects vulnerable. Recently, bug bounty programs, such as `huntr`, have emerged to focus solely on providing bounties to help secure OSS. In this extended abstract, we present preliminary results from an empirical study on GitHub security advisories and `huntr` bug bounty reports, a perspective that is currently understudied because they contain comprehensive information about security incidents, including details about the nature of vulnerabilities, their impact, and how they were resolved and disclosed. Upon scraping within the constraints of the GitHub API and available bug bounty reports, we were able to gather 5,171 security advisories and 3,181 bug bounty reports. Our study includes the following key findings: (1) current review rates cannot keep up with growing unreviewed security advisories; (2) CVEs missing from the National Vulnerability Database prevent alerts from being sent to all affected GitHub projects and external advisory databases; and (3) a majority of projects analyzed do not show previously patched vulnerabilities or enable private vulnerability reporting, leaving gaps in proper disclosure.**

I. Background and Research Questions

To study the state of software vulnerability management, we center our study on one of the largest OSS ecosystems, i.e., GitHub. An OSS ecosystem is made up of open-source project maintainers, vulnerability reporters, and client project developers. GitHub Advisory Database (**GAD**) [1] and the `huntr` bug bounty program [2] help facilitate communication between the different actors in the GitHub OSS ecosystem.

`huntr` is an OSS bug bounty program specifically for GitHub repositories. `huntr` not only pays vulnerability reporters for finding vulnerabilities in GitHub repositories but also pays project maintainers for fixing them. By paying both vulnerability reporters and project maintainers, `huntr` encourages vulnerability reporters to report vulnerabilities and project maintainers to provide the fixes promptly. On the other hand, GAD contains security advisories for publicly disclosed vulnerabilities in GitHub repositories. A GitHub security advisory is a publicly available announcement that discloses a vulnerability fix in a GitHub repository and alerts dependent client projects to update their dependencies.

GAD sources advisories from other public security advisories (e.g., National Vulnerability Database (NVD) [3], FriendsOfPHP security advisories [4]) and those reported on GitHub by project maintainers or vulnerability reporters. The advisories in GAD are divided into two groups: reviewed and unreviewed. Reviewed advisories are reviewed by GitHub, whereas unreviewed advisories are directly published to the database from NVD. Reviewed advisories are further tied to Dependabot where the advisories' dependent client projects are alerted [5]. Such projects are not alerted of unreviewed advisories. Unreviewed advisories that stay unreviewed for a prolonged period can be dangerous for the dependent client projects since the dependent projects may not be aware of the vulnerability fixes, but the advisories detailing the vulnerabilities are available for anyone to view. Although reported vulnerabilities in `huntr` are not available to view until project maintainers provide the fixes, reported vulnerabilities that are not fixed promptly can risk rediscovery by malicious actors. Reported vulnerabilities on either GAD or `huntr` can be assigned a *Common Vulnerabilities and Exposures* (**CVE**).

To understand obstacles that GitHub vulnerabilities face during the vulnerability disclosure process of security advisories from GAD and bug bounty reports from `huntr`, we deduce and investigate the following research questions:

RQ1: What obstacles hinder the exposure of GitHub vulnerabilities from bug bounty reports and security advisories?

RQ2: What do projects from security advisories and bug bounty reports tell us about vulnerability disclosure gaps?

II. Methodology

We organize our study around two key components, security advisories and bug bounty reports. Figure 1 outlines the structure of a representative open-source vulnerability report-and-resolve process in the context of GitHub using GAD, a database containing open-source vulnerabilities, and `huntr`, a bug bounty program focused on GitHub repositories.

As of 09/25/2023, there are 14,588 reviewed security advisories and 197,609 unreviewed security advisories on GAD. Our collected GitHub security advisory sample is a subset of the 14,588 reviewed security advisories, i.e., have both published and reviewed timestamps. Further, security advisory data dates back to October 2017, spanning six years.

Our other data source, `huntr`, does not provide a method of knowing how many bug bounty reports are publicly disclosed, nor a list of projects with existing bug bounty reports. There

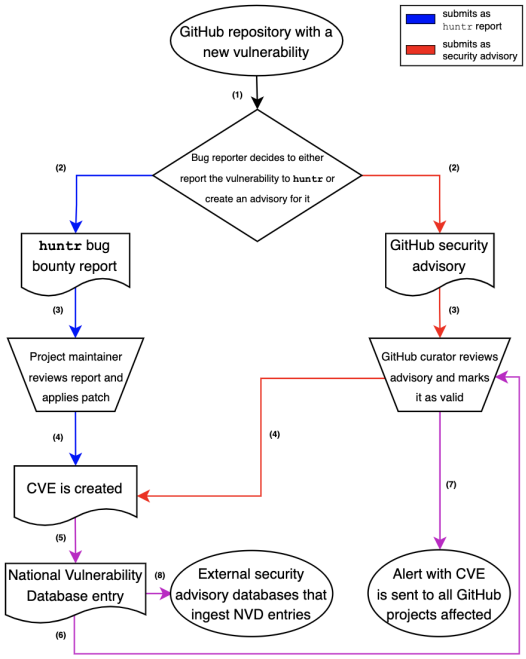


Fig. 1. Two Report-and-Resolve Flows of an Open-source Vulnerability

is a hacktivity page [6] that provides a list of the 100 most recent publicly disclosed bug bounty reports. Our collected bug bounty reports are scraped using the 100 most recent bug reports from each unique project on the `huntr` hacktivity page from 09/01/2021 to 09/30/2023. Bug bounty reports date back to August 2019, spanning four years.

Using all security advisories and bug bounty reports, we identified projects that are linked to GitHub repositories. We then query such repositories directly for the usage of configurable software vulnerability management features. This includes looking for a project vulnerability reporting policy, the "Report a Vulnerability" feature, and public security advisories. For GitHub, a repository's "security policy" provides instructions on how to report a vulnerability, which is much more narrow than the meaning of security policy found in the research literature [7], [8]. Data gathered are as of 09/25/2023.

III. Preliminary Findings

Figure 2 shows the cumulative number of reviewed and unreviewed GitHub security advisories, green and red respectively, over two years. A sudden jump in unreviewed security advisories, starting in May 2022, can be observed as a result of importing thousands of CVE entries from the NVD [9]. Figure 2 suggests that the rate of reviewing security advisories is not fast enough to keep up with unreviewed advisories. Using review rates from our dataset, we find that the average review rate is 5.89 security advisories per day.

Finding 1: If security advisories were halted in November 2023, based on the average review rate of 5.89 per day, it would take approximately 95 years to review all 201,687.

Upon closer inspection of security advisories and bug bounty reports with a corresponding CVE, we find that there are approximately 1.9 times as many missing NVD entries

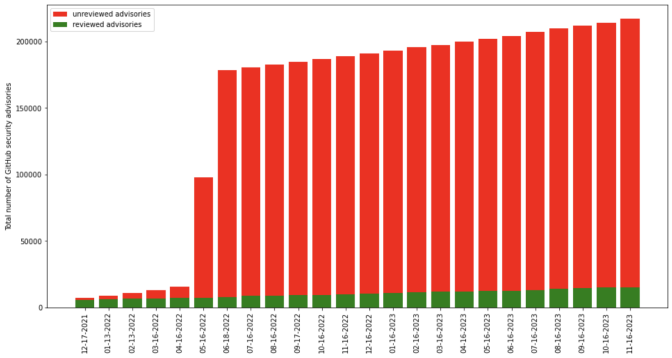


Fig. 2. Number of Reviewed and Unreviewed GitHub Security Advisories Between December 2021 and November 2023

coming from bug bounty reports than from security advisories in our dataset. In other words, it is less likely that a CVE-assigned security advisory has a missing NVD entry, such as "Possible Denial of Service Vulnerability" [10], than a CVE-assigned bug bounty report, such as "Failure to invalidate session after password change" [11], which does not exist in the security advisory database with query "CVE-2022-36029" [1]). This highlights a potential gap in the representation of security vulnerabilities in the NVD, raising concerns about its completeness and reliability.

Finding 2: Although security advisories contain new vulnerabilities less often, 38.6% (1,311/3,392), than bug bounty reports, 98.2% (1,380/1,405), they are streamlined to the NVD 1.8 times faster. CVEs from reports are missing 1.9 times more often in the NVD than CVEs from advisories.

Finding 3: We learn from MITRE that 66.0% (31/47) of CVEs are NVD-absent due to a delay in CNAs publishing them to the CVE List. Such CVEs are halted from reaching external databases that ingest NVD entries.

Further, we report statistics on the lack of software vulnerability management (**SVM**) feature usage in GitHub repositories found from each security advisory and bug bounty report. Security advisories span 1,987 GitHub projects and bug bounty reports span 568 GitHub projects, totaling 2,555 projects.

Finding 4: 52.8% (1,049/1,987) of projects from security advisories have a vulnerability reporting policy. Adding `SECURITY.md` benefits OSS projects as it opens the door for bug reporters that use vulnerability disclosure programs.

Finding 5: 63.5% (1,623/2,555) of projects linked from security advisories and bug bounty reports do not have security advisories publicly displayed. This is a gap in proper vulnerability disclosure as it may hinder awareness of vulnerabilities and mitigation measures for affected projects.

Finding 6: 77.1% (1,969/2,555) of projects linked from security advisories and bug bounties have private vulnerability reporting disabled. This discourages security researchers from responsibly disclosing vulnerabilities. Enabling private vulnerability reporting is easy, but is surprisingly underused.

References

[1] GitHub, "Github security advisory database," https://github.com/advisories, 2017.

[2] A. Nygate, "Huntr," https://huntr.dev, 2020.

[3] NIST, "The national vulnerability database (nvd)," https://nvd.nist.gov/, 1999.

[4] FriendsOfPHP, "Php security advisories," https://github.com/FriendsOfPHP/security-advisories, 2014.

[5] GitHub, "Dependabot: Automated dependency updates built into github," https://github.com/dependabot, 2019.

[6] Huntr, "Hacktivity," https://huntr.dev/bounties/hacktivity/, 2021.

[7] K. Höne and J. H. P. Eloff, "What makes an effective information security policy?" *Network Security*, vol. 2002, no. 6, pp. 14–46, 2002.

[8] M. S. S. Pahnila, and A. Mahmood, "Employees' adherence to information security policies: An empirical study," in *New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007*. IFIP International Federation for Information Processing, vol 232. Springer, 2007, pp. 133–144.

[9] GitHub, "All historical nvd advisories are now listed on github," https://github.blog/changelog/2022-06-08-all-historical-nvd-advisories-are-now-listed-on-github, 2022.

[10] G. Jones, "Possible denial of service vulnerability in rack's header parsing," https://github.com/advisories/GHSA-c6qg-cjj8-47qp, 2023.

[11] C. M. Khanh, "Failure to invalidate session after password change in bigbluebutton/greenlight," https://huntr.dev/bounties/9b341840-fd3f-4a21-839f-ad1fcb422a0e, 2022.

A Glimpse of Vulnerability Disclosure Behaviors and Practices Using GitHub Projects

Jessy Ayala, Yu-Jye Tung, Joshua Garcia – *UC Irvine*

In open-source software (OSS), the number of vulnerabilities has gone ↑↑↑

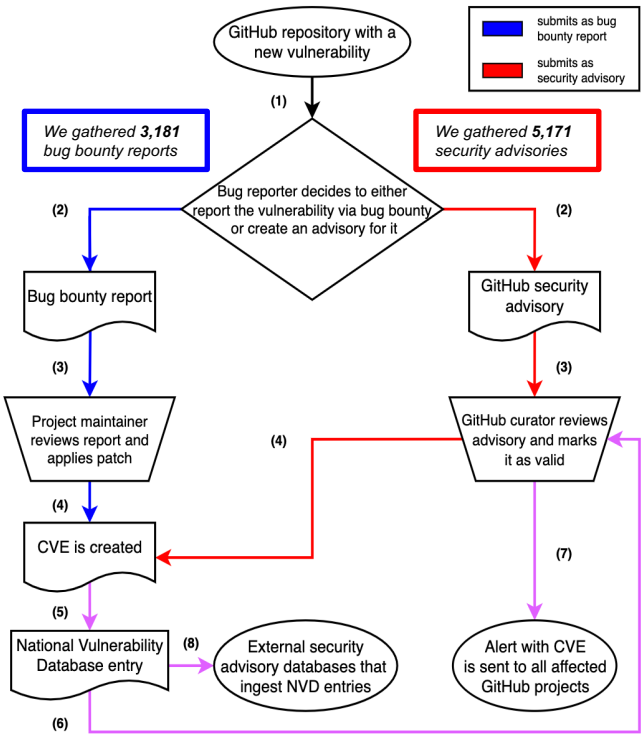
- *Bug bounty reports* can be submitted for open-source projects using bug bounty platforms, e.g., `huntr`, for project maintainers to review vulnerabilities
- GitHub *security advisories* provide a means of sending alerts to projects affected by a vulnerability

Bug bounty reports and security advisories power OSS vulnerability disclosure

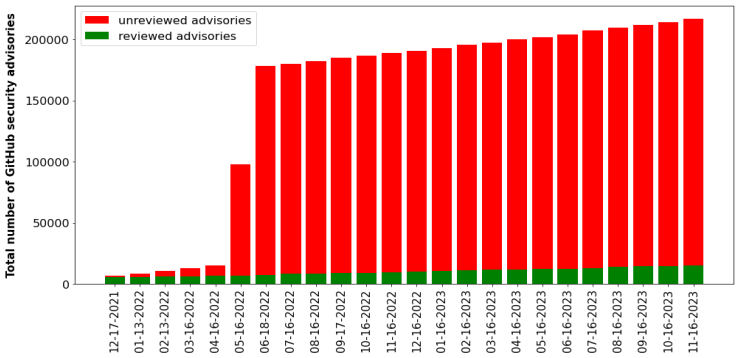
RQ1 What obstacles hinder the exposure of GitHub vulnerabilities from bug bounty reports and security advisories?

RQ2 What do projects from security advisories and bug bounty reports tell us about vulnerability disclosure gaps?

Our model of the ecosystem!



Highlighted Findings from Mining Security Advisories and Bug Bounty Reports



If security advisories were halted in Nov. 2023, based on the avg review rate of 5.9 per day, it would take approximately 95 years to review them all.

Although security advisories contain new vulnerabilities less often, 38.6%, than bug bounty reports, 98.2%, they are NVD-streamlined 1.8x faster.

Vuln. Management Feature Utilized	% of Projects (Security Advisories)	% of Projects (Bug Bounty Reports)
Vuln reporting policy	52.8% (1,049/1,987)	78.7% (447/568)
Public advisories	40.3% (801/1,987)	23.1% (131/568)
Private reporting	23.1% (458/1,987)	22.4% (131/568)

Only 52.8% of projects from security advisories have a vulnerability reporting policy.

63.5% of projects from security advisories & bug bounties don't have advisories publicly displayed.

77.1% of projects from security advisories & bug bounties have private vulnerability reporting disabled.

What's next?

Further analyzing review rates with rigorous statistical techniques

Taking a closer look at how popular projects are affected by missing CVEs

Manually analyzing security advisories & bug bounty reports for trends