Poster: Computer Security Researchers' Experiences with Vulnerability Disclosures

Harshini Sri Ramulu
Paderborn University
Paderborn, Germany
harshini.sri.ramulu@uni-paderborn.de

Anna Lena Rotthaler
Paderborn University
Paderborn, Germany
anna.lena.rotthaler@uni-paderborn.de

Jost Rossel
Paderborn University
Paderborn, Germany
jost.rossel@uni-paderborn.de

Rachel Gonzalez Rodriguez
Paderborn University
Paderborn, Germany
rachel.gonzalez.rodriguez@uni-paderborn.de

Dominik Wermke
North Carolina State University
Raleigh, North Carolina, USA
dwermke@ncsu.edu

Sascha Fahl
CISPA Helmholtz Center for Information Security
Hannover, Germany
fahl@cispa.de

Tadayoshi Kohno
Georgetown University
Washington, D.C., USA
yoshi.kohno@georgetown.edu

Juraj Somorovsky
Paderborn University
Paderborn, Germany
juraj.somorovsky@uni-paderborn.de

Yasemin Acar
Paderborn University & The George Washington University
Paderborn, Germany
yasemin.acar@uni-paderborn.de

Abstract

Vulnerability disclosures are necessary to improve the security of our digital ecosystem. However, they can also be challenging for researchers: it may be hard to find out who the affected parties even are, or how to contact them. Researchers may be ignored or face adversity when disclosing vulnerabilities. We investigate researchers' experiences with vulnerability disclosures, extract best practices, and make recommendations for researchers, institutions that employ them, industry, and regulators to enable effective vulnerability disclosures.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**.

Keywords

software vulnerabilities, vulnerability disclosure, security research

ACM Reference Format:
Harshini Sri Ramulu, Anna Lena Rotthaler, Jost Rossel, Rachel Gonzalez Rodriguez, Dominik Wermke, Sascha Fahl, Tadayoshi Kohno, Juraj Somorovsky, and Yasemin Acar. 2025. Poster: Computer Security Researchers' Experiences with Vulnerability Disclosures. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3719027.3760723

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3760723

1 Introduction

Vulnerability disclosure is critical for software security. In 2024 alone, 39,972 vulnerabilities were reported by NIST National Vulnerability Database (NVD), and 2025 has already more than 28,000 reported vulnerabilities by August 2025 [14]. The external reporting of suspected security vulnerabilities in systems is the last line of defense before these vulnerable systems may get compromised by malicious attackers.

The process of disclosing vulnerabilities to companies and other affected parties—such as software vendors and open-source projects—is usually done through a *'responsible disclosure'* process, where the researchers confidentially disclose to the infected parties and allow sufficient time to fix issues before going public, in a *'coordinated'* disclosure, together with the affected party. If this process does not go smoothly, the systems may remain exposed for an extended time period. Some known challenges include researchers being ignored, not being allowed to publish their findings, or even being sued after disclosing vulnerabilities to companies.

The following research questions guide our research approach:
RQ1: *What is the current status quo of discussing vulnerability disclosures in published research?*
RQ2: *What are the challenges and obstacles faced by security researchers while discovering and disclosing vulnerabilities?*
RQ3: *What are the interactions with the publishing process? What are potential improvements?*

To answer these questions, we analyzed two data sources in parallel, with results from each source informing inquiry in the other source. We collected 1,900 research papers sourced from the top-tier security venues by keyword search, and qualitatively coded their contents for the process surrounding vulnerability disclosure. We also interviewed 22 academic vulnerability researchers with a broad range of expertise and subject areas, focusing on the process

and experiences with vulnerability disclosure. We are subsequently qualitatively analyzing the interviews.

2 Background and Related Work

The reporting of vulnerabilities to vendors and the public has evolved over time [13]. Even though organizations are working on establishing guidelines, a widely accepted guideline or even standard is not yet established [9]. Practices also vary widely across vulnerability types: while cross-site scripting vulnerabilities can be measured and reported at scale [17], high-profile new vulnerabilities, discovered through academic research, might require more skillful disclosures. While disclosures of common vulnerabilities without the goal of academic publication may be supported by bug-bounty programs [7], an established "fits all sizes" process for academic security researchers' disclosures remains elusive. In our study, we aim to understand how *current academic security researchers* experience vulnerability disclosures, what they aim for, and which challenges they encounter, to help establish guidelines *for the security research community*.

Bug bounty programs and vulnerability reward and disclosure programs are well-researched, and several studies have explored the benefits of these programs [1, 4, 6, 9, 12, 15]. Prior work has highlighted the effectiveness of bug bounty programs based on productivity in the number of vulnerabilities reported and the benefits of crowdsourcing [2, 9–11, 15]. Further, Akgul et al. explored bug bounty programs from the perspective of bug hunters and highlighted monetary benefits [3, 18], learning opportunities [16, 18], career flexibility [5], and community benefits as benefits of bug bounty programs [1]. Bug bounty programs also pose challenges with communication, responsiveness, and difficulties with resolving disputes [1]. Further, Fulton et al. highlight that marginalized folks face unique challenges and discrimination related to their identity in vulnerability discovery and reporting [8]. Though our work does not solely focus on bug bounty programs, we aim to understand whether and how security researchers utilize these platforms and explore the challenges and obstacles they encounter while using bug bounty programs.

3 Methods

For the literature review, we used keyword search to collect 1,900 research papers that reported on research that involved finding vulnerabilities. We crawled more than a decade (2012–2024) of published security research papers from four security conferences: ACM CCS, IEEE Security & Privacy, NDSS, and USENIX Security. All papers were ranked based on how often they contained the keywords seen in Table 1. For each paper, we extracted the text containing the keywords (and surrounding context, meaning the paragraph and adjacent sentences) and meta-information, including the title and link to the full text. Four researchers then manually checked the research papers for the inclusion criterion that they discuss a vulnerability, and further analyzed research papers that discussed disclosing the vulnerability.

For the interview study, we interviewed 22 vulnerability researchers. Their research experience ranged from second-year PhD students to retired full professors. They had worked with a wide range of vulnerabilities, including, but not limited to, cryptographic vulnerabilities in hardware, side-channel vulnerabilities in major cryptographic libraries, vulnerabilities in government software, and security-relevant communication software; some vulnerabilities impacted millions of users or even whole ecosystems, and some were of theoretical nature without likely exploits. While many participants also published at cryptography venues, they reported that offensive cryptography research is often more warmly received at security venues, which they therefore target for this area of their research.

Table 1: Keywords used during paper crawl.

Category	Keywords
Vulnerability	vulnerability, vulnerabilities, vulnerable, exploit, CVE
Report	responsible disclosure, disclosure, disclose, vendor response
Bounty	bug bounty, bug bounties, FOSSA, bugcrowd, hackerone, hacker one

4 Preliminary Results

Below we outline our preliminary results of the completed literature review and our ongoing qualitative analysis of interview data.

4.1 Literature review

We find inconsistent reporting, often a lack of reporting of timelines and reactions of those reported to, if any. For someone new to the research area, reading research papers might not help them with effective vulnerability disclosures.

4.2 Interview Study

We outline preliminary interview findings in three areas:

Contacting affected parties. Finding the vendor, or the contact details that will lead to effective communication about the vulnerability is often challenging. Participants reported being unsure who was behind vulnerable devices, not finding contact details, or being ignored or stuck in unproductive discussions with first-level support. We recommend clear pathways to disclose.

Bug bounties. Bug bounties frequently come with a requirement that the timeline for publication is dictated by the affected party—for academic researchers, therefore, participating in a bug bounty program may preclude publishing a research paper.

Effective communication. Researchers may be ignored, or treated adversarially. Participants recommended looping in senior colleagues, having professional websites, and patience and professional communication—for both sides.

5 Outlook

We think that this work, once completed, can inform guidance for effective vulnerability disclosure.

Acknowledgments

We thank all interviewees for their generous participation and in-depth insights.

References

[1] Omer Akgul, Taha Eghtesad, Amit Elazari, Omprakash Gnawali, Jens Grossklags, Michelle L Mazurek, Daniel Votipka, and Aron Laszka. 2023. Bug {Hunters'} Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In *32nd USENIX Security Symposium (USENIX Security 23)*. 2275–2291.

[2] Nikolaos Alexopoulos, Andrew Meneely, Dorian Arnouts, and Max Mühlhäuser. 2021. Who are vulnerability reporters? a large-scale empirical study on floss. In *Proceedings of the 15th ACM/IEEE international symposium on empirical software engineering and measurement (ESEM)*. 1–12.

[3] Abdullah M Algarni and Yashwant K Malaiya. 2013. Most successful vulnerability discoverers: Motivation and methods. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer …, 1.

[4] Soodeh Atefi, Amutheezan Sivagnanam, Afiya Ayman, Jens Grossklags, and Aron Laszka. 2023. The benefits of vulnerability discovery and bug bounty programs: Case studies of Chromium and Firefox. In *Proceedings of the ACM Web Conference 2023*. 2209–2219.

[5] Ryan Ellis and Yuan Stevens. 2022. Bounty everything: Hackers and the making of the global bug marketplace. *Available at SSRN 4009275* (2022).

[6] Matthew Finifter, Devdatta Akhawe, and David Wagner. 2013. An empirical study of vulnerability rewards programs. In *22nd USENIX Security Symposium (USENIX Security 13)*. 273–288.

[7] Huw Fryer and Elena Simperl. 2017. Web science challenges in researching bug bounties. In *Proceedings of the 2017 ACM on Web Science Conference*. 273–277.

[8] Kelsey R Fulton, Samantha Katcher, Kevin Song, Marshini Chetty, Michelle L Mazurek, Chloé Messdaghi, and Daniel Votipka. 2023. Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1997–2014.

[9] Donatello Luna, Luca Allodi, and Marco Cremonini. 2019. Productivity and patterns of activity in bug bounty programs: Analysis of HackerOne and Google vulnerability research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 1–10.

[10] Ana Magazinius, Niklas Mellegård, and Linda Olsson. 2021. What we know about bug bounty programs-an exploratory systematic mapping study. In *Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9*. Springer, 89–106.

[11] Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. 2017. Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity* 3, 2 (2017), 81–90.

[12] Suresh S Malladi and Hemang C Subramanian. 2019. Bug bounty programs for cybersecurity: Practices, issues, and recommendations. *IEEE software* 37, 1 (2019), 31–39.

[13] David McKinney. 2007. Vulnerability bazaar. *IEEE Security & Privacy* 5, 6 (2007), 69–73.

[14] NIST. 2025. National Vulnerability Database. https://nvd.nist.gov/vuln/search#/nvd/home?resultType=statistics. Accessed: 2025-08-12.

[15] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, and Michelle Mazurek. 2018. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 374–391.

[16] Daniel Votipka, Eric Zhang, and Michelle L Mazurek. 2021. Hacked: A pedagogical analysis of online vulnerability discovery exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1268–1285.

[17] Gary Wassermann and Zhendong Su. 2008. Static detection of cross-site scripting vulnerabilities. In *Proceedings of the 30th international conference on Software engineering*. 171–180.

[18] Mingyi Zhao, Jens Grossklags, and Peng Liu. 2015. An empirical study of web vulnerability discovery ecosystems. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*. 1105–1117.