Behind the Curtain: How Shared Hosting Providers Respond to Vulnerability Notifications

Giada Stivala, Rafael Mrowczynski, Maria Hellenthal, Giancarlo Pellegrino
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
stivala.gm@proton.me, {mrowczynski, hellenthal, pellegrino}@cispa.de

***Abstract*—Large-scale vulnerability notifications (VNs) can help hosting provider organizations (HPOs) identify and remediate security vulnerabilities that attackers can exploit in data breaches or phishing campaigns. Previous VN studies have primarily focused on factors under the control of reporters, such as sender reputation, email formatting, and communication channels. Despite these efforts, remediation rates for vulnerability notifications continue to remain consistently low. This paper presents the first in-depth study of how HPOs process vulnerability notifications internally and what organizational and operational factors influence VN effectiveness. We examine the problem from a different perspective to provide the first detailed understanding of the reasons behind persistently low remediation rates. Instead of manipulating parameters of VN campaigns, we interview hosting providers directly, investigating how they handle vulnerability notifications and what factors may influence VN effectiveness, such as VN awareness and reachability, HPOs' service models, and perceived security risks.**

We conducted semi-structured interviews with 24 HPOs across shared hosting and web development services, representing varied company sizes and operator roles. Our findings reveal practical insights on VN processing and abuse workflows. While some providers remain hard to reach due to complex infrastructures, most report routinely handling VNs. However, limited remediation often stems from strict responsibility boundaries, where web application issues are seen as the customer's domain. Low hosting fees and high volumes of daily compromises further discourage both proactive and reactive measures. Our findings show that HPOs blame negligent website owners, and prior works on website owners confirms they often undervalue their sites or lack security know-how. This misalignment raises further concerns about the efficacy of current VN approaches and whether they can reliably prompt remedial action under the existing operational model.

1. Introduction

The security of the Web ecosystem is critical, as vulnerabilities in web services can expose sensitive information and systems to cyberattacks, posing risks not only to website owners but also to hosting companies and other Internet users. A common approach to addressing web vulnerabilities are vulnerability notifications, where the (presumably) responsible party is informed after detection–a practice widely used in large-scale studies by the academic security community. However, identifying and reaching the appropriate contact poses significant challenges, undermining both issue awareness and remediation decisions.

Previous research has extensively explored ways to improve remediation rates for vulnerability notifications by modifying specific properties of VNs, such as email features [1, 2] and sender's attributes [1, 3], the nature and severity of the vulnerability [1, 4, 5], the communication channel [1, 5–8], or the role of the recipient [6, 8–10]. Despite these efforts, the response and remediation rates for notified web vulnerabilities still average between 20 to 30% [1, 2, 6, 8], and no effective alternatives have yet been identified (e.g., still no better channel than WHOIS [6, 8, 11]).

While studies with website owners offered some understanding of their VN evaluation criteria [5, 12], website owners are usually not the recipients of such notifications, as their contacts are not easily available at a large scale. Other studies have explored the causes of non-remediation through interviews with website and system operators [1, 13], revealing a complex landscape. Operators report of multiple undiscovered security misconfigurations that could lead to incidents [14], which underscores the importance of VNs for raising awareness. However, awareness alone does not guarantee remediation [1], suggesting that factors beyond VN characteristics influence these decisions. Further research examined whether technical or organizational factors impacted remediation but found no single factor to be more significant than others [13]. As a result, we still lack a clear understanding of what happens after a vulnerability notification is received, as none of the previous works has investigated the internal processes of the receiving entities.

To address this gap, we turn our focus to hosting provider organizations, which frequently receive vulnerability notifications due to their accessible contact information and capacity to intervene in affected customer instances. To our best knowledge, this is the first study to deeply investigate how HPOs internally receive, process, and respond to vulnerability notifications, providing a previously missing perspective on these workflows. Our first objective

is to examine how these notifications are handled from the receiver's side, offering insights into the features and processes that researchers have so far only hypothesized. Our second, and main, objective is to identify the organizational and operational factors, beyond the characteristics of the notifications themselves, that influence IT operators at HPOs in their decision to remediate. To answer our research questions, we conducted a qualitative study based on semi-structured interviews with 24 IT operators working within HPOs, covering shared hosting providers and web agencies of varying sizes and service models. Rather than focusing on the design of notification campaigns, our study explores how HPOs receive, interpret, and act on vulnerability notifications in practice, from the inside.

Our findings show that while most providers are aware of and routinely handle VNs, remediation is often deprioritized due to clearly defined service boundaries, operational cost considerations, and the perception that responsibility lies with customers. Providers generally take responsibility for managing infrastructure and removing abusive content such as phishing, malware, or illegal material. However, they see the underlying causes of such abuse, lying in the security of web applications, as the responsibility of customers or their web agencies. Moreover, we find that organizational flexibility, rather than rigid processes, characterizes how notifications are handled, with decisions frequently left to individual operators. Although reachability issues persist in some multi-layered hosting setups, most providers can be contacted through established channels. Ultimately, our results suggest that the limited effectiveness of VNs is not due to technical or procedural obstacles, but to a misalignment between the goals of security researchers and the business logic of hosting providers. This disconnect is deepened by providers' frustration with what they describe as widespread negligence among website owners, raising doubts about the viability of remediation within the current shared hosting ecosystem.

2. Background and Methods

Our investigation was driven by the observed low remediation rates to web vulnerability notifications and our desire to uncover the roadblocks that prevent addressing these problems. Against this background, we investigate:

RQ1: *How are vulnerability notifications received and processed within HPOs?*

RQ2: *What are the characteristics of HPOs (their internal factors) that influence their VN-handling and the respective remediation processes?*

To answer these research questions, we first conducted a content analysis of HPO websites. This analysis provided a map of the research field and informed the development of our sampling strategy. Using this strategy, we then carried out a qualitative study based on semi-structured interviews with individuals owning or working for small- to large-sized hosting provider companies. The interviews focused on VN remediation both in detail and from a broader perspective, while allowing participants to share their own viewpoints.

Data analysis and interpretation of the interview study were carried out using a combination of Qualitative Content Analysis [15–17], a top-down approach, with some components of Grounded Theory [18–20] which operates in an inductive, bottom-up manner [21]. We used this two-pronged approach to systematically identify patterns and themes in our interviews. On the one hand, we aimed at superficially known but understudied aspects of hosting activities as reflected in our interview-guide questions and corresponding codes. On the other hand, the bottom-up component allowed us to identify phenomena which have not been noticed by previous research.

2.1. Sampling Outline

Our sampling strategy followed the general principle of maximal structural variation [22], with the aim of capturing diverse behavior across providers offering different combinations of services. The goal was to expand the surface of investigation with respect to our main research focus: interventions following vulnerability notifications. We approached this from two angles. First, we considered the potential for hosting provider intervention. Different types of hosting services imply varying degrees of provider control [23]. For instance, shared hosting typically grants customers fewer privileges while leaving a larger portion of the technical infrastructure under the HPO's control, compared to dedicated hosting. Second, we scoped our study to services known for suffering high levels of abuse, as these are more likely to receive vulnerability notifications. This supported our focus on the broader category of shared hosting services, which consistently show particularly high concentrations of abuse [23–25]. From this framing, we derived two key HPO characteristics likely to influence remediation behavior: the type of shared hosting service (e.g., web application, VPS) and the level of service management (managed vs. unmanaged). These two dimensions formed the basis of a sampling matrix, which we used to map the hosting landscape and identify specific providers for interview recruitment.

2.1.1. Mapping the Landscape of Hosting Services. We manually compiled a list of hosting provider organizations. Using corporate datasets [26–28] was prohibitively expensive, and identifying organizations via IPs or Autonomous Systems from ranked website lists (e.g.,[29, 30]) was discarded due to bias toward global providers. Instead, we identified companies by analyzing discussions on relevant Reddit communities (r/VPS, r/agency, r/webhosting, r/Hosting). Posts were selected if they discussed hosting services, excluded if tagged as advertisements or focused on out-of-scope topics. This process yielded 150 posts and a preliminary list of 197 companies.

Next, we manually reviewed the websites of these companies, discarding those offering only out-of-scope services or that no longer existed. Using a top-down content analysis of advertised services, we mapped offerings into the sampling matrix (service types and management). This map served then as the basis for our sampling process, as

we anticipated that perspectives on VN remediation would vary across different segments. To capture this variation, we aimed to interview representatives from organizations operating in diverse areas of the hosting landscape. After this review, we finalized a list of 175 companies with a total of 716 distinct offerings (available at [31]), spanning six high-level categories of hosting services. These are Dedicated Server, Virtual Private Server, Reseller Hosting, Shared Hosting, Website Builder, Web Agency.

Hosting Services and VNs in Scope. In this work, we consider VNs reporting issues as web application code vulnerabilities [1, 8, 10], misconfigurations [2, 32, 33], or internet services abuse, such as malware, phishing, or SEO infections [3, 12, 34, 35]. Consequently, our focus is on hosting services and providers operating closer to the application layer, such as VPS providers, shared hosting providers, and web agencies.

2.1.2. Web Hosting Services. Hosting services in scope can be categorized in three high-level types, here ordered by required technical expertise.

Virtual Private Servers (VPS) offer dedicated portions of shared server resources, ensuring better performance and scalability but requiring higher technical expertise for setup and maintenance. *Shared hosting* involves instead multiple users sharing a single server's resources, such as bandwidth, CPU, and memory, ensuring affordability and simplicity for website owners. Website setup is facilitated through graphical interfaces, making the service accessible even to users with low technical skills.

Web agencies (or "resellers") act as intermediaries between end-users and hosting infrastructure. Their revenue comes from developing and managing websites, with customization being central to their business model. The term has a dual meaning: "reseller hosting" refers to a service offered by HPOs, while "web agencies" are the businesses using this service to deliver final products to customers.

Hosting services may be either managed or unmanaged. *Managed hosting* services include provider assistance, for example with configuration or maintenance, as defined in service agreements, while *unmanaged hosting* leaves these responsibilities to the client. The level of management is closely tied to the underlying hosting type and can also vary across providers, as per their terms of service. For a VPS, management may focus on low-level tasks, such as operating system updates. In contrast, managed shared hosting often extends to application-layer services, such as website setup and configuration, catering to less technically proficient users.

2.1.3. Recruitment. We used the service data to group companies by similar offerings. We represented each company's services as a one-hot-encoded vector and applied the k-modes clustering algorithm to group them, using an empirically-chosen value of $k = 13$ for an optimal balance of interpretability and granularity. Our clustering results mirrored the distribution of services in our dataset, where the majority (78%) of companies provide more than one service in various combinations. We obtained five clusters of HPOs offering primarily one service (e.g., website builder, web agency), and eight clusters where HPOs either offered combinations of two or three services (e.g., shared hosting and VPS) or were primarily centered on one service with additional, less significant offerings.

We chose to start from companies offering a single service to reduce the complexity of HPO characteristics that could influence VN remediation. This decision was based on our categorization of service offerings and management. We recruited participants using a mix of cold-calling via available contacts (phone, email, ticketing portal, or chat, resulting in nine participants), snowballing and personal contact networks (still guided by our sampling map, resulting in nine participants), and professional social networks (as LinkedIn, resulting in six participants). This resulted in a total of 24 hosting providers and web agencies from eleven countries. We describe hosting providers and individual participants in Section 2.5 and Table 1.

2.2. Interviewing Procedure

Following established methodological recommendations for semi-structured interviews [36, 37], we developed an interview guide as a flexible framework to steer the data collection process. The primary aim was to explore if and how hosting provider organizations handle vulnerability notifications. Thus, a large portion of the guide addressed VNs, investigating employee awareness, communication channels, and decision-making processes.

Recognizing that VN handling may be shaped by broader factors, we included sections examining technical factors (e.g., infrastructure and tools), business factors (e.g., provided services and management), and organizational factors (e.g., internal procedures and management priorities) [14, 38, 39]. To familiarize ourselves with industry procedures for security management, we relied on the NIST Computer Security Incident Handling Guide [40], which helped shape questions on identified assets, perceived risks, and operational aspects, such as the use of playbooks (step-by-step procedures for employees) and the involvement of third-party entities in incident response. We report the complete interview guide in Appendix A.

The interview guide was tested in two pilot interviews with hosting-acquainted colleagues at our research institution. The guide was iteratively refined throughout the study by incorporating insights from earlier interviews to partly re-focus on some newly emergent, relevant issues. For instance, some questions were tailored based on whether the interviewee was a classical hosting provider or part of a web agency. When participants spontaneously introduced some of the topics in the course of the interview, we followed their lead allowing for a change in the order of discussed topics. However, the interview guide always contained a stable core of topics we discussed with all our participants throughout our entire study. While we initially posed broad questions to avoid biasing responses, the data ultimately stem from participant responses concerning application-level

vulnerability notifications; participants who did not engage with these were considered unfamiliar with VNs, and the rare mentions of other notification types (e.g., OS or network) were excluded from the analysis as out of scope. This approach aligns with best practices in qualitative research, which emphasize adaptability to enrich data quality.

Nearly all interviews were conducted via Zoom[1] between Aug '24 and June '25, lasting between 60 and 90 minutes. Before the interview, all participants completed a questionnaire providing consent, demographic details, and information about their HPO, reported in Table 2. All interviews were audio-recorded and transcribed using our in-house AI-based transcription tool. Most interviews were conducted in English, with some in Italian later translated for data processing (four via DeepL and three via our in-house AI-based transcription tool). All interview transcripts were anonymized by removing personal and HPO-specific information.

2.3. Data Analysis

The analysis of interview data combined a top-down approach of Qualitative Content Analysis [15–17] with elements of Grouded Theory's bottom-up methodology [18–20]. An initial set of codes was derived from the topical areas and specific questions in our interview guide. It was clear from the very beginning that our interviewees talked about these issues, because we explicitly asked them about it. To avoid fully subsuming our rich data under predetermined categories, we also allowed for the creation of new codes in a bottom-up manner inspired by Grounded Theory's open-coding procedure. This approach enabled us to capture specificity and novelty emerging from the data while anchoring it within the broader topical areas represented by the initial top-down codes [21].

Initially, three researchers (a computer scientist, a psychologist and a sociologist) independently coded four transcripts to identify discrete text units relevant to the research questions. To ensure consistency and resolve interpretive differences, we collaboratively reviewed and refined the initial codes through detailed discussions, fostering shared understanding and adapting codes as necessary. We did not calculate inter-coder agreement rate as our final agreement on codings approached 100% [41–44].

Following this, the researchers conducted several iterations of descriptive coding, grouping open codes into broader thematic categories. This iterative process led to the development of increasingly abstract categories that captured key themes and patterns in the data, resulting in a preliminary codebook. The codebook was then applied to five additional interviews, during which it was tested, refined, and expanded to include omitted codes, ensuring comprehensive data coverage. Finally, we used the finalized codebook (Appendix B) to code the remaining fifteen interviews, with all coding performed using ATLAS.ti [45].

1. One interview was conducted in person due to the proximity of HPO's premises to the location of our research institution.

We conducted interviews until all HPO clusters identified via the mapping procedure were covered, and our analysis indicated saturation in identifying and describing phenomena relevant to the research questions. By the end of this process, no new themes or problems emerged, confirming that the studied phenomenon and its diversity were comprehensively described. The final code system was then used for a category-driven re-examination of the primary data. A comparative matrix was created to extract RQ-relevant information from each interview, enabling the identification of similarities and differences in how individual HPOs addressed the problems focused by our research questions.

2.4. Ethical considerations

During the recruitment phase, we ensured that each company was contacted only once. If no interest was expressed, the company was excluded from further follow-up. Additionally, we sent a maximum of two reminders to potential interviewees who showed interest.

We conducted the interviews via videotelephony, but only recorded audio tracks. These audio files were used exclusively for transcription and were deleted after the transcription was completed. To protect participant confidentiality, we kept demographic data and personally identifiable information (e.g., details collected during recruitment) strictly separate from the study data. Personally identifiable information was deleted upon completion of the data-gathering phase. Anonymity was preserved through the assignment of unique participant ID numbers and the use of password-protected spreadsheets accessible only to the principal investigators. Additionally, transcripts were fully anonymized to remove references to individuals, company names, specific locations, associated organizations, and any identifiable tools or products developed by the company.

All participants provided informed consent prior to their involvement. As compensation, we offered each participant 50 USD. Further, the responsible ERB for our institution reviewed and approved our study procedure.

2.5. Participant Data and HPO Information

Our interview study included 24 participants from eleven different countries, reported in Table 1. Participants represented a wide variety of positions and represented companies varying significantly in size, ranging from small (less than 10 employees, nine companies) to mid-sized (11–50, 51–200, 201–1,000, twelve companies) to large (over 1,000 employees, three companies). Participants demonstrated very diverse technical skillsets tied to their roles. In a nutshell, their tasks can be divided in three categories: leaders (ten participants), customer-facing (seven participants), and backend roles (seven participants).

Regarding the services offered, the study captured a wide range of market coverage, reported in Table 2. Web application hosting services ("shared hosting") were the most common, provided by 12 companies. Eight companies offered VPS solutions, while four operated as web agencies.

HPO ID	HPO size	CySec dept. or person	Primary education	Current role	Age	YoE	Years in HPO	Multiple HPOs	Country
WA-M-1	11-50	●	Computer Science	Front-end dev., Proj. Manager	29	7	1-3	⋆	IT
WA-M-2	51-200	●	Computer Science	System Operator	24	2.5	4-10		DE
WA-M-3	1-10	□	Computer Science	CEO	41	10	11-20		IT
WA-U-1	1-10	●	Industrial electronics	Responsible Executive	59	24	11-20		IT
SH-M-1	1-10	◇	Computer Science	Owner	23	7	4-10		NL
SH-M-2	201-1000	▲	Media and Film	Product Owner	37	7	4-10		BG
SH-M-3	11-50	▲	Computer Science	Customer Success Engineer	32	4	4-10		IN
SH-M-4	51-200	●	Electronics and Telecomm.	Technical support executive	25	3	1-3		IN
SH-M-5	>1000	▲	Computer Animation	Digital Fraud Analyst	42	8	11-20		USA
SH-M-6	11-50	▲	Computer Science	CTO	42	11	>20		BG
SH-M-7	201-1000	▲	History	CEO	37	20	1-3		UK
SH-U-1	1-10	□	Telecommunications	CEO	45	27	>20		DE
SH-U-2	11-50	□	Computer Science	Developer	29	10	4-10		DE
SH-U-3	51-200	▲	Computer Science	Technical Support	27	7	1-3	3	PH
SH-U-4	1-10	□	Computer Science	CEO & CTO	38	22	>20		AT
SH-MU-1	>1000	▲	Computer Science	Linux System Administrator	26	5	<1	2	IT
VPS-M-1	11-50	▲	Computer Science	Cloud Administrator	37	5	4-10		IT
VPS-U-1	1-10	□	Did not attend university	Owner	45	22	>20		DE
VPS-U-2	11-50	▲	Business and economics	Operations and maintenance		10	4-10		IT
VPS-U-3	51-200	◇	Computer Science	System Administrator	31	5	1-3		IT
VPS-U-4	1-10	□	Computer Science	Customer Success Manager	19	2	1-3		PL
VPS-U-5	1-10	-	High School Diploma	CEO	19	2	1-3		IN
VPS-MU-1	>1000	▲	Computer Science	Senior Network Engineer	28	10	<1	⋆	DE
VPS-MU-2	1-10	●	Communication	CEO	42	20	4-10		DK

TABLE 1: Participant details collected via survey. Legend for *HPO ID*: [Type]-[Mgmt]-[ID], where: Type: WA = Web Agency, SH = Shared (Web Application) Hosting, VPS = VPS. Mgmt: M = Managed, U = Unmanaged, MU = Both. ID: incremental number. Legend for *CySec dept.*: ● participant; ◇ another employee; □ collective decision; ▲ HPO security/abuse department; - no department/employee. Legend for *Multiple HPOs*: ⋆ for previous employer only, or total number N of employers discussed. Note: participant's country may differ from the HPO's, e.g., for global enterprises.

Managed services	VPS	Reseller Hosting	Shared Hosting	Web Agency
Managed	*VPS-M-1*, *VPS-MU-1*, *VPS-MU-2*, *SH-MU-1*, *SH-M-4*, *SH-M-6*	*SH-M-2*, *SH-M-3*, *SH-M-4*, *SH-M-5*, *SH-M-6*	*SH-M-1*, *SH-M-2*, *SH-M-3*, *SH-M-4*, *SH-M-5*, *SH-M-6*, *SH-M-7*, *VPS-M-1*	*WA-M-1*, *WA-M-2*, *WA-M-3*
Unmanaged	*VPS-U-1*, *VPS-U-2*, *VPS-U-3*, *VPS-U-4*, *VPS-U-5*, *VPS-MU-1*, *SH-U-4*	*SH-U-2*, *SH-U-4*, *VPS-U-1*, *VPS-U-2*, *VPS-MU-2*	*SH-U-1*, *SH-U-2*, *SH-U-3*, *VPS-U-3*	*WA-U-1*
Management outside contract	*VPS-MU-1*, *VPS-MU-2*		*SH-U-1*, *SH-U-2*, *SH-U-4*, *SH-MU-1*	

TABLE 2: Distribution of HPOs' services by support levels (rows) and service types (cols). The row *management outside of contract* is a new finding, absent from initial market mapping.

When examining the nature of hosting management, the split was almost even: eleven companies provided managed hosting, while ten operated on an unmanaged basis, and three offered both options.

While most participants focused on a single company during the interview, four offered insights into more than one. Two of them (*WA-M-1*, *VPS-MU-1*, marked with ⋆ in Table 1) discussed previous employers, which were more relevant to our study than their current roles. The remaining two reported experiences from multiple companies: *SH-U-3* referenced three organizations, and *SH-MU-1* discussed two. None of the HPOs discussed by these participants overlapped with those described by others. We noted partial overlap between *VPS-U-1* and *SH-U-2*, as *SH-U-2* is a spin-off from *VPS-U-1*, established to diversify their product offerings. Moreover, we remark that the service categorizations reported in Table 2 follow the companies' self-descriptions, though their actual offerings and management levels vary and are not always consistent across companies. Lastly, *VPS-U-3* is a non-profit organization in the education sector, whose services align closely with those of typical hosting provider organizations, while *SH-U-3* and *SH-MU-1* both provide registrar services alongside of hosting.

2.6. Structure of Findings

The following sections 3 through 6 address our research questions with case-specific examples and conclude with key takeaways. Section 7 discusses main findings, offers actionable insights for future notifications, and suggests directions for further research. We use « angular parentheses » to report verbatim quotes from interviews.

3. Notification Channel and Message

This section presents our findings on the unprompted communications received by HPOs from external actors regarding the security and privacy of their infrastructure or hosted customer instances, addressing the first part of **RQ1** on *How are vulnerability notifications received*. Our questions focused on factors explored in prior work, such as reachability and email characteristics, while allowing participants to share their experiences with all forms of unprompted communication.

3.1. Receiving VNs

3.1.1. Awareness of VNs. All but three participants (*WA-M-1*, *VPS-M-1*, *SH-M-3*) were familiar with the concept of vulnerability notification. Most participants regularly engaged with them (e.g., *SH-M-1*, *SH-U-1*, *WA-M-2*, *VPS-U-1*, *VPS-MU-1*, *SH-MU-1*) and had a positive or neutral view of this mean of communication. Conversely, a subset of participants expressed skepticism regarding the intent of VN senders (*WA-M-3*), or doubted that external actors could identify vulnerabilities they were not already aware of (*VPS-U-3*, *SH-M-2*). For others, the idea of receiving notifications from *unrelated* third parties was unfamiliar, expecting to receive vulnerability reports only from established business relationships or trusted communication channels (*VPS-M-1*, *SH-M-3*, *VPS-U-5*).

3.1.2. Reachability. Participants were asked about the channels available for external actors to report VNs. Responses highlighted seven distinct communication endpoints and six different channels, with some participants identifying multiple methods.

WHOIS was the most frequently mentioned channel (seven HPOs), primarily among organizations managing their own infrastructure. One large company reported primarily receiving machine-readable abuse reports as a paid service, and two more reported preferring submissions via the company portal. Interestingly, one VPS provider reported only receiving abuse notifications through their provider, as they rent all infrastructure and don't own any IPs.

Web agencies provided contact details either in website credits or on a separate page, such as an "Impressum" or a `security.txt` file (one agency). None relied on WHOIS for communication. Small web agencies focusing on website development and management relied heavily on their hosting providers to inform them of issues, often due to a lack of in-house expertise or lack of alignment with their business model and setup (*WA-M-1*, *WA-M-3*).

3.2. Content and Sender Characteristics

3.2.1. Senders of VNs. HPOs receive security-related communications from a diverse range of senders. Eight participants reported receiving notifications regularly from various entities, which can be grouped into three main categories.

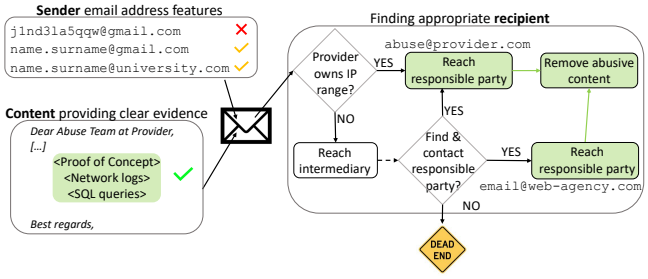

Figure 1: VN creation process based on provider feedback. The sender's email is only relevant if it raises red flags; the body's evidence is most important. On the left, the diagram shows how the email's routing depends on the recipient: if the HPO owns the IP range (per WHOIS), they can be contacted directly. Otherwise, the VN is sent to the infrastructure provider (i.e., the IP range owner, e.g., a data center or cloud provider), who acts as an intermediary and must forward the message to the affected HPO.

First, four participants (*SH-U-2*, *VPS-U-1*, *VPS-MU-1*, *SH-U-3*) mentioned receiving security advisories or investigation requests from government agencies, CERTs, or police departments. Then, four participants mentioned established commercial companies focused on spam, malware, phishing (e.g., Netcraft), or legal issues as brand protection and DMCA reports. These senders were seen as reliable and their notifications were generally addressed promptly due to their established reputations.

Three participants reported receiving reports from private individuals, referred to as « white hat hackers » (*WA-M-2*) or « technician[s] » (derogatory, *WA-M-3*). However, opinions on these reports were divided. While some participants appreciated these notifications, others found it challenging to distinguish genuine reports from unsubstantiated claims or requests for monetary compensation. One participant summarized the skepticism: « ["Security researcher"] is not an official protected term, a lot of people call themselves security researcher, which might be the 14 year old from Bangalore who thinks revealing the web service version number is dangerous » (*VPS-U-1*). Several participants, including both small and large HPOs, reported experiencing high volumes of spam in their VN inboxes. The cause remained unclear, as both affected and unaffected participants used spam filters and public `abuse@` addresses. Abuse reports from private individuals were uncommon: only three participants recalled interactions with academics, while others mentioned cases involving individuals directly affected by abuse on their platforms, such as victims of DDoS attacks or impersonation.

3.2.2. Email Content and Metadata. Among participants familiar with VNs, the criteria for evaluating reports were a key discussion point. While prior work highlighted email features (style, tone, metadata), most participants downplayed their importance. Only a few preferred formal email addresses; most based decisions on technical content, priori-

tizing reports with evidence (e.g., logs or Proof-of-Concept), and directly examined of the reported website. *WA-M-3*, *WA-M-2*, and *VPS-MU-2* report receiving emails from private addresses, raising suspicion: « [T]his is a cryptic email address [...]. So everything looks really, really phishy. And afterwards you say, okay, thanks for your report » (*WA-M-2*). *VPS-MU-2* also addressed the case of random email addresses, which prompted extra scrutiny: « Some people [...] send it from some random streaming of characters @gmail.com. In which case, we take a look at it a little bit closer ». In summary, most providers accept personal email addresses, but emails from random-looking senders are examined more critically, with the final assessment based on the report's content.

Takeaways. Our findings do not indicate significant roadblocks concerning awareness and posture towards VNs. While we observed that reachability can be an issue, given by hosting setups involving middle layers as registrars, resellers, and outsourced services, most providers still indicated WHOIS as the right source for their contacts. Figure 1 illustrates the creation of a VN based on the feedback from our providers. Providers reported being contacted regularly by security companies, which creates established communication channels and patterns. Rarely receiving notifications from individuals, such as researchers, might impact HPOs' perceptions of these communications, potentially making them more suspicious. However, participants noted that reports including strong evidence of issues were always considered, regardless of sender reputation and email metadata.

4. VN Handling Procedures

This section examines the internal processes triggered when a security issue is detected or reported to an HPO, addressing the second part of **RQ1** on *How are vulnerability notifications processed*. Participants described how security event management was handled in their organizations, including the roles and responsibilities of security teams, remediation procedures, internal communication protocols, and interactions with customers or external stakeholders.

4.1. Internal Handling Procedures

HPOs can adopt structured methods to ensure consistent handling of common problems, sometimes referred to as "playbooks", though the level of formalization varies significantly. We investigated the presence of formalized procedures regulating vulnerability notification handling.

We observed that most providers do not follow a strict or formalized process for handling vulnerability notifications, though some have more structured approaches than others. For example, operators at *VPS-MU-1* and *SH-M-5* create playbooks for managing security events as part of their regular tasks, while *SH-MU-1* reported having a playbook to address VN reports at their previous employer. Other HPOs standardized interventions in customer spaces via internal « wikis » (e.g., *SH-U-1*, *SH-M-2*, *SH-M-3*, *SH-U-3*).

Most participants described having minimal or no formal guidelines for handling security events. For example, at *WA-M-2*, security decisions are made based on log interpretations, while at *SH-M-2* and *SH-MU-1*, operators are encouraged to address issues leveraging their own skills. *VPS-U-1*, also owner of a spin-off, *SH-U-2*, relies on a habitualized [46] cybersecurity awareness grounded in his employees' professional socialization within tech-savvy hacktivist backgrounds or open-source programmer communities. Thus, they are assumed to be highly sensitive to S&P topics: « The majority of my team members are coming from like hacker spaces and generally the open source community. And they already have a deeply ingrained approach, they discover security problems in open source software on a daily basis and handle them in appropriate ways. And I think they do this in the best and most responsible way ».

4.1.1. Impact of Internal Organizational Structures. We interviewed IT professionals across a wide range of roles, including executives, abuse analysts, and support staff, from both small and large hosting providers, ensuring a diverse and balanced perspective across organizational scales. This diversity allowed us to examine who handles VNs, the steps involved, and the interactions among professionals within hosting organizations. This was particularly evident in larger companies, where specialization and compartmentalization are more common. In such cases, VNs are typically managed by a dedicated abuse department with access to the `abuse@` mailbox. These operators evaluate VNs in a self-contained process that rarely involves other departments, and may also develop internal playbooks for handling specific types of application-level abuse. When VNs involve legal concerns, as fraud or DMCA complaints, they may be forwarded to the legal department. In rare instances, when VNs relate to infrastructural issues, such as those at the IP level, the abuse team may collaborate with infrastructure-focused employees, such as DevOps or Site Reliability Engineers.

Customer support also plays a role in abuse handling as the first point of contact for clients. While most interactions involve routine setup or configuration, support agents may occasionally assist clients affected by exploits. In complex cases, and where company structure permits, support staff can escalate issues to more experienced personnel, such as "Level 2 support" or the abuse team. However, in practice, the two departments usually operate independently. Participants reported no interdepartmental friction or procedural obstacles in addressing VNs. In smaller companies, roles are often consolidated, with a single employee managing the entire process.

4.1.2. Procedures Established by Certifications. Certifications are formal attestations granted by recognized standardization bodies, indicating that an organization's processes or products meet specific industry requirements. When a

company certifies its procedures or software, it means these have been evaluated and shown to comply with the defined criteria of the relevant standard (e.g., ISO/IEC 27001 for information security management). Certification can apply to all internal procedures or only selected ones, depending on organizational priorities. In this context, we sought to determine whether holding certifications related to security or incident response had any impact on how HPOs manage VN handling. Few participants (*VPS-MU-1*, *VPS-M-1*, *SH-MU-1*) reported getting one or more certifications to access specific market segments, such as public administration (*VPS-MU-1*, *SH-MU-1*) or Limited Liability Companies (*VPS-M-1*). « We are about to take the ISO 27001 certification, [...] Because, you know, it is fundamental for this type of thing. [...] Because, above all, customers ask for it » (*VPS-M-1*). Certifications were however not mentioned as a factor playing in procedures for remediating issues or vulnerabilities in customer spaces, situations for which participants reported following other legal frameworks (especially nation state's or GDPR). These participants reported certifying procedures such as « datacenter encryption » (*VPS-MU-1*) or « SLA requirements and disaster recovery » (*VPS-M-1*). Notably, *WA-U-1*, a web agency developing software for the public administration, reported having no constraint on the application software.

4.2. Procedures Involving External Stakeholders

We examined potential remediation challenges arising from a multi-stakeholder setup. Participants did not report dependencies on external entities involved in remediation, such as CERTs or Managed Security Service Providers.

4.2.1. Interactions between Hosting Providers, Web Agencies, and Final Customers. One notable multi-stakeholder dynamic is the "reseller hosting" model (introduced in Section 2.1.2). We investigated the responsibility and authorizational boundaries between hosting providers and their clients ("resellers", or web agencies). *SH-M-2* and *SH-M-3*, both managed hosting providers, described their admin panel as having a fine-grained access control system that enables both intermediaries (web agencies) and end-users (web agency clients) to act within customer spaces, effectively removing authorization barriers. While this paints a positive picture, none of the web agencies outsourcing hosting (*WA-M-1*, *WA-U-1*, *WA-M-3*) reported using managed shared hosting. Instead, they preferred service packages without customer support, shifting the burden of remediation to themselves. A few participants described a strict authorization boundary in both directions (e.g., *SH-M-1*, *SH-M-6*, *WA-M-2*, *WA-U-1*). Hosting providers noted that some resellers enforce clear separation of responsibilities (« We do not interfere there, and actually many of them do not allow us to touch [their] products », *SH-M-6*). Conversely, web agencies reported losing contact with clients after the initial website development, as ongoing management was transferred to the client's internal IT department.

Finally, web agencies (e.g., *WA-M-2*, *WA-M-3*) might experience issues when onboarding of customers with externally developed websites. In such cases, *WA-M-3* notes that their typical solution is to freeze the codebase until the customer agrees to pay for a complete rewrite, even if the website runs outdated or vulnerable code.

4.2.2. Procedures at Registrars. Domain registrars are companies authorized to manage the reservation of internet domain names and typically operate separately from hosting providers. In cases of abuse, registrars may receive complaints related to domain ownership or misuse, where they can react by, e.g., disabling domain resolution by web clients. However, enforcement actions like content removal fall under the responsibility of hosting providers.

Two participants, *SH-U-3* and *SH-MU-1*, also acted as domain registrars, providing unique insights absent from accounts by other interviewees. We report their valuable insights, acknowledging the limited generalizability. The participants reported checking all incoming emails, regardless of sender or email features, considering as only criterion whether the domain or content was under their control. Providers reported taking immediate action in case the domain hosted illegal material (e.g., phishing, copyright violations, child pornography, or other breaches of local law), suspending the domain and notifying both customer and hosting provider. For all other types of issues, HPO behaviors differed depending on their business model: *SH-U-3*, offering unmanaged services, left the website untouched, even if obviously compromised. *SH-MU-1*, offering both managed and unmanaged services, evaluated whether the reported flaw posed risks to infrastructure stability, other customers' instances, or sensitive data security. If none of these applied and the customer was not a premium client, they sent an email notification to the client without further action.

Takeaways. Few HPOs reported having a clearly defined process outlining specific steps and criteria for handling vulnerability notifications, while most of them follow semi-formalized procedures which participants generally describe as flexible and not limiting to their operations. Handling of incoming reports is typically left to the discretion of individual operators, where most rely on unwritten but commonly followed rules. Internal HPO structure and division of responsibilities was not reported as a roadblock by participants working in medium to large HPOs. Few hosting providers reported having clear authorization boundaries when dealing with web agencies as intermediaries, in which cases they cannot take action directly and simply forward the received VN. Most web agencies confirmed that they rely on hosting providers to be informed about website issues.

5. Deciding Whether to Intervene

After establishing that some VNs are received and that handling procedures are often informal, we asked participants what actions they would take and why, addressing **RQ2**. Their decision-making criteria largely fell into three categories, outlined below. Participants also reported challenges in determining whether to intervene, as well as exceptional circumstances that prompt remediation.

5.1. Type of Vulnerability or Issue

We investigated whether the type of reported vulnerability influenced providers' remediation decisions. In general, action was taken when there was evidence of ongoing malicious activity, such as phishing, spam, malware delivery, or distribution of illegal content. Almost all participants reported they would respond by removing the malicious content, and potentially blocking parts of the website or taking the website offline. Additionally, they notified affected customers, using methods ranging from simple alerts to more engaged outreach prompting customer-side remediation.

Alerts concerning *potential* exploits, such as vulnerabilities in web applications, were treated differently. VPS providers, whether managed or unmanaged, stated they were not contractually obligated to oversee application software installed by customers, even when deployed using tools provided by the HPO. As a result, they did not address security and privacy issues at the application layer. This approach was described by *SH-U-2* as « the infrastructure-customer divide », defining the boundary of responsibility between provider and customer. These providers focused on maintaining infrastructure stability by managing elements such as operating systems, databases, and programming environments, and responded to reports involving Denial of Service, port scanning, or email spam, but drew a firm line at application-level issues.

In the case of shared hosting, unmanaged providers described a hands-off approach to all web application concerns, stating « it's basically out of scope for us to take care of that [...]. Then you've got a shell there. Have fun. » (*SH-U-2*). Managed service providers expressed a similar stance: « You get a place where you do not think of operating system upgrades, control panel upgrades, compatibility issues, [...] everything is covered. But it's that's where we our job ends and it's your responsibility to upload the software and after that to update it and keep it to date and safe » (*SH-M-6*). This underscores a strict division of responsibility between hosting infrastructure and code management, further echoed by another provider: « [But if] the issue with the application [is] like, in the coding, so we do not provide any development-related support » (*SH-M-4*).

Operators reported two reasons behind this approach: first, the low cost of their offerings, which does not compensate for the time spent remediating and, additionally, the « bajillion » tickets they need to deal with daily (*SH-M-5*), requiring them to minimize the time spent for each of them.

5.2. Legal Constraints

Legal obligations play a significant role in motivating hosting providers to take action. For example, there are cases where the operator must apply a patch or update to avoid legal liability, or instead, they refrain from intervening, even when capable, because taking action could expose them to legal liability. Two examples illustrate these dynamics. Participants generally reported no awareness of legal requirements concerning the maintenance of hosting infrastructure or software. *SH-MU-1*, for instance, confirmed the absence of such regulations but emphasized that existing laws do penalize service providers in the event of a data breach. To reduce this risk, the company has adopted an internal update policy aimed at preventing incidents that could lead to legal consequences: « [T]here is no law that tells you that all systems must be in the last stable version, but clearly it tells you that if, because of the system, [because of] a vulnerability... personal data, sensitive data, and so on, get stolen, you are responsible » (*SH-MU-1*).

The second example concerns unmanaged contracts. In these cases, the legal obligation typically extends only to notifying the client about the issue (e.g., *SH-U-1*, *WA-M-2*, *SH-U-3*, *SH-M-6*). Once the report is delivered, responsibility shifts to the client, and the operator is no longer involved. Applying code patches or modifying incompatible modules is not only unnecessarily costly when the issue does not affect others, but also risky, especially for highly customized setups. An unfamiliar operator might unintentionally break the site: « [I]n the [BUSINESS UNIT] where I am, there are about 50 people more or less, and the clients are.. hundreds of thousands... so... Understanding and taking action on every single personalization that can be done on the various websites, CMS websites [...] would be madness. » (*SH-MU-1*). As a result, proactive remediation is not an option, since making changes would make the operator legally responsible. In managed contracts, when customers request a fix, some operators may choose to intervene but require the customer to sign a waiver before making any changes to the hosting environment.

5.3. Customer-Specific Factors and Interactions

5.3.1. Interactions with Customers. In some cases, customers react to vulnerability notifications and reach back to their hosting providers. Participants expressed mixed feelings about customers raising such issues (e.g., *SH-U-1*, *WA-M-2*, *WA-M-3*). They frequently reported that customers lacked the necessary understanding, demanded significant time for explanations, and created an unnecessary burden on their operations. Customer service is particularly costly for providers, creating challenges for both unmanaged and managed hosting services. Many HPOs face risks of financial losses due to the high cost of support agents relative to their low prices.

Many HPOs (e.g., *SH-U-1*, *WA-M-2*, *VPS-U-2*, *VPS-MU-1*) report that customers are often unwilling to pay security services (e.g., website cleanup). To mitigate this,

providers like *SH-U-2* and *VPS-U-1* focus heavily on creating detailed wiki articles to assist customers, without direct support, while *SH-M-2* requires users to consult their knowledge base before contacting support: « [I]f everybody comes to tickets, our tech support team will be simply overwhelmed » (*SH-M-2*).

5.3.2. Management Defined by Contract. Companies offering unmanaged services limit customer support actions to written suggestions, such as troubleshooting steps or links to online resources (e.g., *SH-U-2*, *SH-U-3*). A few of them reported expectations mismatches with customers on the level of management happen, usually solved via polite explanations (*SH-U-2*, *VPS-U-1*) or by proposing additional paid services (e.g., *WA-M-2*, *SH-MU-1*, *SH-M-7*), with some, like *SH-U-3*, upselling services with sales-based bonuses. Managed service providers offered broader support, though intervention typically required a customer request and varied broadly by provider. Support agents often demonstrated goodwill in helping customers by updating software (e.g., *WA-M-1*, *SH-M-1*), restoring backups, or removing affected content upon request (e.g., *VPS-M-1*, *SH-M-2*, *SH-M-3*). No provider mentioned actively inspecting for vulnerabilities, and only one (*WA-M-1*) reported reviewing plugin code to ensure functionality.

Code-level remediation was rare and generally offered when contractual services included custom web application development (*SH-M-1*, *WA-M-3*, *VPS-MU-1*, *WA-M-2*). For example, *WA-M-3* described a complex, manual remediation of a hacked WordPress site redirecting visitors to malicious content. This intervention followed a customer complaint triggered by a Google SafeBrowsing warning. However, the same provider admitted to ignoring outdated PHP versions with known vulnerabilities and websites lacking HTTPS. This suggests that customer involvement may have strongly influenced their decision to act.

Conversely, business concerns might motivate providers not to address security issues. For instance, *WA-M-2* and *WA-M-3* develop custom software, generating revenue by offering improvements as new product features. *WA-M-3* notes that while their custom CMS is regularly updated and patched, updates are withheld from customers due to their unique customizations and to encourage them to purchase updated installations.

5.3.3. Exceptional Proactive Remediation. Occasionally, hosting providers take proactive measures to address compromised customer instances without waiting for them to reach back. These actions, such as disabling compromised websites or sections of them, are taken to safeguard the overall infrastructure's security and ensure fair resource allocation among all customers. This approach is often necessary because customers are slow to respond to notifications (e.g., *SH-U-1*, *SH-U-2*, *VPS-U-1*, *SH-MU-1*).

The motivations for such proactive efforts are often rooted in business strategy. For example, *SH-U-1* emphasizes high-quality customer service as a key differentiator but seeks to reduce time-intensive customer calls by addressing issues proactively. *VPS-MU-1*, which blends managed and unmanaged services, may exceed their contractual obligations to maintain goodwill and strengthen customer relationships–a decision driven by their administrative department. *SH-U-2*, *VPS-U-1*, and *VPS-MU-2* on the other hand, may proactively address compromised customer instances out of a commitment to prevent internet abuse, a stance shaped by their organizational and ethical principles: « We consider this as part of our responsibility that we not only have for our customers, but also for the rest of the internet. We don't want our machines to attack other machines » (*VPS-U-1*).

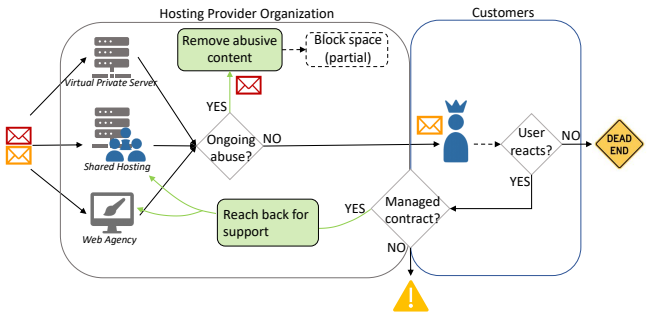

Figure 2: Notification handling workflow. Incoming reports are analyzed by abuse teams and abusive content taken down, with further actions depending on the HPO. Reports are otherwise forwarded to customers, and escalation to customer support depend on user action and contract terms.

Takeaways. Figure 2 illustrates the VN handling workflow that emerged from our interviews. Most providers indicated their abuse team promptly addresses abuse such as phishing, malware delivery, or distribution of illegal content, regardless of the type of hosting and of the degree of service management. Reports concerning other types of web-application issues are forwarded to customers. In fact, our findings reveal a common understanding of service boundaries: customers, or web agencies in their stance, are responsible for code maintenance, while hosting providers focus on infrastructure and service availability. Moreover, the type of service provided affects the level of customer support, with some providers supporting users in remediations to a larger extent. Finally, providers are also influenced by factors that extend beyond the content of the VN, as the company's ethical position on addressing internet abuse, the perceived value of long-term customer satisfaction, and the motivations of individual support agents.

6. The Role of VNs in Infrastructure Security

While most hosting providers do receive vulnerability notifications, our earlier findings indicate that these are

often not prioritized in practice, highlighting a misalignment between provider security goals and those of researchers. To better understand this disconnect, we examined providers' awareness of abuse within their infrastructure, the security measures they employ at a technical level, and their perceptions of risk related to compromised customer instances.

6.1. Provider Awareness of Abuse and Security

We began by examining the extent to which hosting providers are aware of abuse and of the security posture of their customers operating on their infrastructure. Our goal was to assess whether visibility given by VNs could offer providers insights they currently lack, demonstrating practical value in enhancing their situational awareness.

Most hosting providers focus on maintaining visibility and control over their infrastructure to ensure reliable service and uphold service-level agreements. Providers who own their hardware (e.g., *SH-M-6*, *SH-MU-1*, *WA-M-2*, *VPS-U-3*, *VPS-MU-2*) typically implement routines that monitor network activity, I/O, RAM, and other resource usage. For some, these monitoring systems also serve as early warnings for potential security incidents, but it usually falls to a skilled operator to determine if unusual activity reflects legitimate use or malicious behavior (*WA-M-2*). HPOs that do not manage their own hardware (e.g., *WA-M-1*, *WA-U-1*, *WA-M-3*, *VPS-U-5*) often depend on tools supplied by their upstream hosting partners, using these to gain some operational insight. In some cases, structured monitoring is minimal or absent, with providers relying mainly on customer reports to identify problems (*WA-M-3*, *VPS-U-4*).

Overall, the primary goal of monitoring is to maintain infrastructure performance, not to detect abuse or assess the security of customer spaces. As a result, if customer instances are compromised but do not disrupt service or exceed expected resource usage, these incidents frequently go unnoticed and unaddressed. Only a minority of providers report actively assessing the security posture of their customers' environments (*SH-U-1*, *SH-M-2*).

6.1.1. Securing Hosting Infrastructure. Most providers secure their infrastructure's by employing protections such as DDoS mitigation, firewalls, and isolated virtual networks (*VPS-U-2*, *VPS-M-1*). Many use Linux permissions and least privilege principles to prevent customer infections from escalating (*SH-U-1*, *SH-U-2*, *VPS-U-1*), though implementation varies widely based on provider size and whether hosting is in-house or outsourced. Only few providers monitor for abuse higher up the stack, with some reducing risk by by preventing web app code edits: « the WordPress code itself is locked. Like no one can edit it. [...] So that's something that is totally secure and locked down » (*SH-M-3*). Alternatively, hosting providers use web application firewalls, or run signature-based file scans (*SH-M-1*, *SH-U-1*). Web agencies may also deploy code-level protections (*WA-U-1*, *WA-M-3*).

6.2. Perception of Risk from Customer Spaces

HPOs described a range of technical measures used to secure their infrastructure, with a primary focus on ensuring resilience and service continuity. Because their responses centered on infrastructure security, we examined their perceptions of risks associated with customer spaces. Our goal was to understand the reasons behind their limited engagement, including whether this results from a perceived low risk or deliberate trade-offs.

6.2.1. Perceived Risk from Customer Instances. Customer instance compromise is common, « we see WordPress exploits the whole time », as *SH-M-7* reports. However, providers expressed confidence in their infrastructure's ability to contain such incidents, keeping systems stable and functional. As *VPS-U-1* noted, « our infrastructure does not care about phishing ». Only one participant, *WA-M-1*, recounted a full compromise of their hosting space after they transitioned to a less managed setup to meet the demands of a larger client.

VPS instances are typically compromised due to customer misconfigurations or are acquired directly for illicit use (e.g., *VPS-MU-1*, *VPS-U-2*, *VPS-MU-2*). In shared hosting, abuse often stems from outdated websites and plugins, malicious uploads, cracked plugins, or weak or leaked admin passwords. Although attacks on popular open-source web applications are well known, providers continue to support them and deal with the resulting abuse. For example, *WA-M-3* accommodates customers who request WordPress sites, despite acknowledging they are frequent targets: « [E]very now and then we get that client who insists on having WordPress no matter what, so, to avoid losing the client or the project during the quote phase... ».

Web agencies expressed a different perception of risk compared to shared hosting and VPS providers. For them, the main concern is protecting data, as they see little incentive for attackers to target custom code given the high cost and low potential gain. *WA-M-3* believes that custom-built web applications are inherently secure due to their unique nature, leveraging a form of "security by obscurity". *WA-M-2* similarly claims they have never had a hacked website, although they experienced a sophisticated data exfiltration attack. While custom code can reduce exposure to automated attacks, *WA-M-3* and *WA-M-2* also acknowledged that it introduces risks from implementation flaws and overlooked interactions. Nonetheless, they believe the resources required to test for vulnerabilities across many customized deployments are not economically justifiable.

Finally, risk perception also depends on what providers consider worth protecting. *WA-M-3* for instance, disregards HTTPS implementation on sites they believe contain nothing valuable. Similarly, *VPS-U-2* suggests that security should reflect business value, stating that loose measures are fine if all you are protecting is « three fishbones and four sandwiches ».

Ultimately, we found that most providers in our study shared a similar philosophy, particularly those offering low-

cost, standardized hosting services through public sign-up processes. In contrast, two providers primarily serving large businesses or public administration (*VPS-MU-1*, *VPS-M-1*), as well as one with a mixed clientele (*SH-MU-1*), demonstrated significantly greater attention to security. These providers described remediation processes that addressed more complex threats than typical WordPress compromises.

Our findings suggest that most hosting providers view customer instance compromise as posing minimal risk, considering proactive application-layer security systems as an optional enhancement rather than a necessity. Providers frequently targeted by low-sophistication attackers, such as "script kiddies", may be particularly likely to hold this view. In contrast, providers who implement comprehensive security measures tend to face more sophisticated threats and do not rely on standardized setups commonly targeted by automated attacks. This, in turn, may reinforce the disconnect observed with vulnerability notifications among the former group, as security in these hosting environments is regarded as an added benefit rather than a core requirement.

Takeaways. The security posture of hosting providers is shaped primarily by operational priorities and the need to protect their own infrastructure, rather than by concerns for individual customer environments. Resource monitoring is primarily intended to maintain service level agreements and manage legal risks, and any detection of abuse within customer spaces tends to be incidental rather than the result of targeted efforts. Providers generally express confidence in their technical safeguards to isolate issues and protect core systems. This aligns with and reinforces their passive stance towards application-level vulnerability notifications.

7. Discussion

We conducted and analyzed semi-structured interviews to explore why hosting provider organizations often fail to remediate reported vulnerabilities. Our analysis focused on how vulnerability notifications are received and handled (**RQ1**), identifying the underlying criteria behind the limited remediation responses commonly noted by researchers (**RQ2**). This section summarizes our findings and future directions based on insights from our 24 participants.

7.1. Comparison with Prior Works

We investigated impactful factors highlighted by prior works, such as contact channels, email content, and features of the sender, as well as HPOs' internal structures, analyzing whether and to what extent they contribute to the lack of VN remediation.

First, our study revisits the reachability issues observed in previous work [6, 8, 11]. In fact, most hosting providers confirmed that their contact is available via WHOIS, for example through ARIN [47] or RIPE [48] databases. However, the issue of reachability persists when expanding the scope to actors not considered in prior studies, such as web agencies, who may have an actual impact on remediating reported issues. Additionally, trust plays a different role than in earlier research, which emphasized general distrust [1, 5, 12]. Our participants noted that clear, technical emails with credible explanations are usually considered, though not always acted upon. Finally, while prior research emphasized inner-organizational technical and structural barriers to secure practices [14, 49–51], and challenges with keeping systems up-to-date [38, 52–54], participants in our study reported no major roadblocks in managing their own infrastructure, suggesting that these factors are less critical for VN remediation [13]. The observed lack of remediation was explained by hosting providers as a result of the nature of the vulnerability, often viewed as outside the provider's responsibility. This new framing also helps explain why operator awareness did not always lead to remediation [1, 2, 13, 55].

Notably, the reasons reported by operators differ from those described in [56], which investigates the lack of patching following vulnerability reporting in Dutch municipalities. While the concept of responsibility is central in both works, Ethembabaoglu et al. attribute non-patching to a lack of awareness leading to neglect [56], whereas our study shows that remediation in commercial hosting providers is often refused based on contractual terms. In web agencies, remediation is only partially implemented, depending on business-related factors.

7.2. Implications and Future Directions

7.2.1. VNs as a Source of Awareness. We thoroughly investigated the technical infrastructure and security measures at hosting providers. Most providers believe their infrastructure is resilient to malicious activity occurring in customer environments. As a result, and sometimes also due to their large customer base, many providers do not closely monitor ongoing abuse or enforce remediation. Previous works also observed the lack of proactive remediation by HPOs [10] which, complemented with website owners' neglect or forgetfulness concerning the security posture of their websites [9, 57], underscores the relevance of vulnerability notification campaigns, which help fight internet abuse at scale, raising HPOs' awareness.

7.2.2. Improving on Reachability. The most straightforward, though not necessarily more effective, approach to increase remediation rates may be to notify those actually responsible. Identifying website owners at scale remains a well-known challenge [1, 5]. To overcome this, researchers could explore more advanced automated methods for identifying contact points, selecting appropriate targets such as website owners or web agencies based on the issue type. Future work could involve AI agents capable of navigating websites [58], locating contact information, and extracting relevant text. However, researchers should consider that

many end users do not hire professionals to maintain their websites. The content of vulnerability notifications should therefore be tailored to the recipient, as prior studies have shown that end users interpret such messages very differently [12, 59].

At the same time, successful large-scale vulnerability notification has been shown to be feasible through paid services [60]. This raises a broader question about whether the challenge lies in the lack of a standardized infrastructure available to researchers. Future work could address this by developing a shared contact database, similarly to the development of Tranco [30] as an alternative to Alexa 1 Million, in order to reduce the impact of limited reachability on remediation outcomes.

7.2.3. Lowering Cost of Remediation for Providers. Many providers expressed a cynical view of the current state of abuse in shared hosting, where hackers compromise hundreds of sites with a single click and website owners are described as unskilled and careless, both in managing websites and in valuing website data. Especially among website hosting providers, the volume of daily abuse tickets was reported to be overwhelming (similarly to [61]), leaving little room for careful attention to individual cases. A few providers mentioned occasionally resolving issues proactively, not out of policy but to avoid more costly customer service calls. Still, increasing staff to handle abuse reports more thoroughly appears impractical, as it would require raising prices in a highly cost-sensitive market.

Although providers set pretty strict responsibility boundaries, researchers could focus on making remediation easier and less resource-intensive for them. Many providers value technical detail, suggesting that notifications including clear evidence of the issue and detailed remediation steps could lead to higher response rates.

Moreover, while simply updating the web application software is sometimes the most effective and straightforward remediation, this is often not feasible, as updates can cause incompatibilities with plugins. Our study shows that in such cases, providers often choose not to take action. Previous studies have shown that end users may be unaware of the need to update or may be unwilling to do so when updates impair website functionality [57]. This issue is further complicated by the open-source nature of many free web application tools, which are often untested or no longer maintained. In such situations, researchers who discover the problem could help identify stable versions of the software to which updates are possible, or recommend alternative software that maintains overall functionality. End users, who often prioritize functionality over security, may otherwise never seek such alternatives, possibly due to a lack of awareness of the associated security risks.

7.2.4. Beyond Reachability: Bridging Responsibility Gaps. While improving the reachability of vulnerability notifications remains an important step, our findings caution against treating it as a silver bullet. Simply reaching more providers does not guarantee remediation [1, 13], as awareness alone rarely triggers remediation when responsibility is perceived to lie elsewhere. Instead, our study highlights a systemic gap: researchers expose risks, providers host the affected system yet reject ownership of the vulnerabilities, and end users–who are formally responsible–are often unaware, disinterested, or unmotivated to act [57]. Future work should focus on mechanisms that balance these competing positions, such as approaches that increase end-user awareness of downstream risks or tools that empower providers to intervene in compromised sites without alienating customers or incurring prohibitive costs. Ultimately, improving remediation will require not just better messages, but a better alignment of incentives across all three types of actors.

7.3. Limitations

The field of research on vulnerability notification is broad, and our study does not aim to cover all possible scenarios. We focused specifically on web application vulnerabilities, whereas responses may differ for issues affecting HPO infrastructure, lower layers of the Internet stack, or internet-connected devices. We did not examine hosting services such as Dedicated Servers, Colocation, and Website Builders. These were excluded due to the nature of provider involvement in each case. Dedicated Servers and Colocation offer an extremely high degree of user control, with minimal provider intervention, while Website Builders represent the opposite extreme, offering limited customization through provider-specific, closed-source platforms. Our sample thus covers segments where providers retain some responsibility for the hosted software environment (shared hosting, VPS, and web agencies). While some VPS offerings may resemble dedicated-server models with little provider involvement, others involve substantial management by the provider. As with most qualitative work, our findings are not statistically generalizable, e.g., to all parts of the hosting ecosystem, but aim for transferability by providing in-depth accounts across a diverse sample, reflecting structural variation in the hosting providers population studied.

Secondly, we interviewed only one participant per HPO, potentially missing other perspectives on security in larger organizations. Despite our efforts, recruiting proved challenging. While interviewees provided valuable insights into company practices, future studies should conduct multiple interviews within the same HPOs to better capture inner-organizational dynamics of dealing with cy-sec issues and VN handling. Additionally, while we acknowledge that many providers in our sample are Europe-based, we remark that there was no such selection criteria on our side, and that this is merely a result of the choice of participants willing to respond to our messages.

We also acknowledge that our study relies on participants' accounts rather than direct observation, and we did not experimentally validate providers' claims. While we observed no signs of intentional withholding during interviews, some providers may not have been fully transparent about their practices for reputational reasons. Nonetheless, several

participants openly discussed faulty systems or overlooked organizational procedures, suggesting a willingness to go beyond idealized accounts. Finally, our study may be influenced by opt-in as well as social desirability biases, and demand effects. To minimize these, we avoided disclosing the study's exact focus on security and privacy topic during recruitment, encouraging open discussion and reducing bias related to prior VN experiences.

8. Conclusion

This study shifts the lens of vulnerability notification research by examining the recipients–hosting provider organizations–rather than optimizing the reporting process. To our best knowledge, this is the first study to deeply investigate how HPOs internally process and respond to vulnerability notifications. Through interviews with 24 HPOs, we find that while most providers are reachable and familiar with handling VNs, remediation remains limited due to structural and economic factors rather than technical ones.

Our findings indicate that low remediation rates are not primarily caused by unreachability, distrust, or internal procedural barriers. Instead, they stem from clear service boundaries, where responsibility for code vulnerabilities lies outside the scope of hosting providers' obligations. Cost considerations, the commoditized nature of hosting services, and the perceived insignificance of individual customer environments further reduce the incentive to act. Moreover, remediation decisions are shaped by business priorities, ethical stances, and the discretion of individual operators rather than systematic security policies.

These insights challenge existing assumptions in VN literature and suggest that improving remediation rates requires addressing the underlying misalignment between the security goals of external reporters and the service logic of HPOs. Improving reachability remains important, especially by better targeting responsible parties such as website owners or web agencies. Yet the limited skills and engagement of many website owners complicate notification efforts, highlighting the need for messages tailored to non-experts.

References

[1] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, "Didn't you hear me?—towards more successful web vulnerability notifications," in *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS)*, 2018.

[2] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, "You've got vulnerability: Exploring effective vulnerability notifications," in *25th USENIX Security Symposium*, 2016.

[3] O. Cetin, M. Hanif Jhaveri, C. Gañán, M. van Eeten, and T. Moore, "Understanding the role of sender reputation in abuse reporting and cleanup," *Journal of Cybersecurity*, 2016.

[4] C. Utz, M. Michels, M. Degeling, N. Marnau, and B. Stock, "Comparing large-scale privacy and security notifications," *Proceedings on Privacy Enhancing Technologies*, 2023.

[5] M. Maass, A. Stöver, H. Pridöhl, S. Bretthauer, D. Herrmann, M. Hollick, and I. Spiecker, "Effective notification campaigns on the web: A matter of trust, framing, and support," in *30th USENIX Security Symposium*, 2021.

[6] O. Cetin, C. Ganan, M. Korczynski, and M. Van Eeten, "Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning," in *Workshop on the Economics of Information Security (WEIS)*, 2017.

[7] M. Maaß, M.-P. Clement, and M. Hollick, "Snail mail beats email any day:on effective operator security notifications in the internet," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021.

[8] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, you have a problem: On the feasibility of {Large-Scale} web vulnerability notification," in *25th USENIX Security Symposium*, 2016.

[9] A. Stöver, N. Gerber, H. Pridöhl, M. Maass, S. Bretthauer, M. Hollick, D. Herrmann *et al.*, "How website owners face privacy issues: Thematic analysis of responses from a covert notification study reveals diverse circumstances and challenges," *Proceedings on Privacy Enhancing Technologies*, 2023.

[10] D. Canali, D. Balzarotti, and A. Francillon, "The role of web hosting providers in detecting compromised websites," in *Proceedings of the 22nd international conference on World Wide Web*, 2013.

[11] T. Poteat and F. Li, "Who you gonna call? an empirical evaluation of website security. txt deployment," in *Proceedings of the 21st ACM Internet Measurement Conference*, 2021.

[12] A. Hennig, F. Neusser, A. A. Pawelek, D. Herrmann, and P. Mayer, "Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications," in *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 2022.

[13] T. Bondar, H. Assal, and A. Abdou, "Why do internet devices remain vulnerable? a survey with system administrators," in *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2023). NDSS*, 2023.

[14] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, "Investigating system operators' perspective on security misconfigurations," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*.

[15] P. Mayring, "Qualitative content analysis," *Forum: Qualitative Sozialforschung / Forum: Qualitative Social Research*, vol. 1, no. 2, p. Art. 20, 2000.

[16] M. Schreier, *Qualitative Content Analysis in Practice*. Los Angeles and London and New Delhi and Singapore and Washington D.C.: Sage, 2012.

[17] ——, "Qualitative content analysis," in *The SAGE*

Handbook of Qualitative Data Analysis, U. Flick, Ed. Los Angeles and London and New Delhi and Singapore and Washington DC: Sage, 2014, pp. 170–183.

[18] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company, 1967.

[19] K. C. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. Thousand Oaks, Calif.: Sage, 2006.

[20] A. L. Strauss and J. M. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed. Thousand Oaks, Calif.: Sage Publications, 2008.

[21] J. Saldaña, "Coding and analysis strategies," in *The Oxford Handbook of Qualitative Research*, P. Leavy, Ed. Oxford: Oxford University Press, 2014.

[22] G. Kleining, "Umriss zu einer methodologie qualitativer sozialforschung," *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, no. 34, pp. 224–253, 1982.

[23] S. Tajalizadehkhoob, T. Van Goethem, M. Korczyński, A. Noroozian, R. Böhme, T. Moore, W. Joosen, and M. Van Eeten, "Herding vulnerable cats: a statistical approach to disentangle joint responsibility for web security in shared hosting," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.

[24] APWG, "The global phishing survey: Trends and domain name use in 2016," https://docs.apwg.org//reports/APWG_Global_Phishing_Report_2015-2016.pdf?_ga=2.220159775.701668710.1639446174-1616809074.1639170127, 2016.

[25] S. Tajalizadehkhoob, M. Korczyński, A. Noroozian, C. Ganan, and M. Van Eeten, "Apples, oranges and hosting providers: Heterogeneity and security in the hosting market," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*.

[26] OpenCorporates, https://opencorporates.com/.

[27] Crunchbase, http://crunchbase.com.

[28] Dun & Bradstreet, https://www.dnb.com/.

[29] K. Ruth, D. Kumar, B. Wang, L. Valenta, and Z. Durumeric, "Toppling top lists: Evaluating the accuracy of popular website lists," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022.

[30] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen, "Tranco: A research-oriented top sites ranking hardened against manipulation," 2019.

[31] , "Hosting hosting provider market landscape – section 2.1.1," https://doi.org/10.5281/zenodo.17160673, 2025.

[32] S. Pletinckx, K. Borgolte, and T. Fiebig, "Out of sight, out of mind: Detecting orphaned web pages at internet-scale," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*.

[33] S. Roth, T. Barron, S. Calzavara, N. Nikiforakis, and B. Stock, "Complex security policy? a longitudinal analysis of deployed content security policies," in *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS)*, 2020.

[34] M. Vasek and T. Moore, "Do malware reports expedite cleanup? an experimental study." USENIX Association, 2012.

[35] G. Stivala, G. De Stefano, A. Mengascini, M. Graziano, and G. Pellegrino, "Uncovering the role of support infrastructure in clickbait pdf campaigns," in *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)*, 2024.

[36] J. Lazar, J. H. Feng, and H. Hochheiser, *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[37] A. Witzel and H. Reiter, *The Problem-Centred Interview: Principles and Practice*. SAGE Publications Ltd, 2012.

[38] F. Li, L. Rogers, A. Mathur, N. Malkin, and M. Chetty, "Keepers of the machines: Examining how system administrators manage software updates for multiple machines," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[39] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding it security professionals and their tools," in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007.

[40] P. Cichonski, T. Millar, T. Grance, K. Scarfone *et al.*, "Computer security incident handling guide," *NIST Special Publication*, 2012.

[41] P. Klostermeyer, S. Amft, S. Höltervennhoff, A. Krause, N. Busch, and S. Fahl, "Skipping the security side quests: A qualitative study on security practices and challenges in game development," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024.

[42] S. Klivan, S. Höltervennhoff, R. Panskus, K. Marky, and S. Fahl, "Everyone for themselves? a qualitative study about individual security setups of open source software contributors," in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024.

[43] N. Huaman, J. Suray, J. H. Klemmer, M. Fourné, S. Klivan, I. Trummová, Y. Acar, and S. Fahl, ""you have to read 50 different {RFCs} that contradict each other": An interview study on the experiences of implementing cryptographic standards," in *33rd USENIX Security Symposium*, 2024.

[44] J. Schmüser, H. Sri Ramulu, N. Wöhler, C. Stransky, F. Bensmann, D. Dimitrov, S. Schellhammer, D. Wermke, S. Dietze, Y. Acar *et al.*, "Analyzing security and privacy advice during the 2022 russian invasion of ukraine on twitter," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024.

[45] ATLAS.ti GmbH, "Atlas.ti | the #1 software for qualitative data analysis. online," https://atlasti.com/.

[46] P. Bourdieu, *Outline of a Theory of Practice.* Cambridge University Press, 1977.

[47] ARIN, "American Registry for Internet Numbers,"

https://www.arin.net/.
[48] RIPE, "RIPE NCC," https://www.ripe.net/.
[49] N. Huaman, B. von Skarczinski, C. Stransky, D. Wermke, Y. Acar, A. Dreißigacker, and S. Fahl, "A {Large-Scale} interview study on information security in and attacks against small and medium-sized enterprises," in *30th USENIX Security Symposium*, 2021.
[50] J. Staddon and N. Easterday, ""it's a generally exhausting field" a large-scale study of security incident management workflows and pain points," in *2019 17th International Conference on Privacy, Security and Trust (PST)*, 2019.
[51] N. Alomar, P. Wijesekera, E. Qiu, and S. Egelman, ""you've got your nice list of bugs, now what?" vulnerability discovery and management processes in the wild," in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*.
[52] C. Tiefenau, M. Häring, K. Krombholz, and E. Von Zezschwitz, "Security, availability, and multiple information sources: Exploring update behavior of system administrators," in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*.
[53] A. D. Jenkins, L. Liu, M. K. Wolters, and K. Vaniea, "Not as easy as just update: Survey of system administrators and patching behaviours," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024.
[54] F. Martius and C. Tiefenau, "What does this update do to my systems?–an analysis of the importance of update-related information to system administrators," in *Workshop on Security Information Workers, WSIW*, 2020.
[55] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey *et al.*, "The matter of heartbleed," in *Proceedings of the 2014 conference on internet measurement conference*, 2014.
[56] A. Ethembabaoglu, R. van Wegberg, Y. Zhauniarovich, and M. van Eeten, "The unpatchables: Why municipalities persist in running vulnerable hosts," in *33rd USENIX Security Symposium*, 2024.
[57] M. Hellenthal, L. Gotsche, R. Mrowczynski, S. Kugel, M. Schilling, and B. Stock, "The (un) usual suspects–studying reasons for lacking updates in wordpress," in *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS)*, 2025.
[58] A. Stafeev, T. Recktenwald, G. De Stefano, S. Khodayari, and G. Pellegrino, "Yurascanner: Leveraging llms for task-driven web app scanning," in *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS)*, 2024.
[59] A. Hennig, N. T. T. Vuong, and P. Mayer, "Vision: What the hack is going on? a first look at how website owners became aware that their website was hacked," in *Proceedings of the 2023 European Symposium on Usable Security*, 2023.
[60] G. C. M. Moura, T. Daniels, M. Bosteels, S. Castro, M. Müller, T. Wabeke, T. van den Hout, M. Korczyński, and G. Smaragdakis, "Characterizing and mitigating phishing attacks at cctld scale," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024.
[61] S. de Smale, R. van Dijk, X. Bouwman, J. van der Ham, and M. van Eeten, "No one drinks from the firehose: How organizations filter and prioritize vulnerability information," in *2023 IEEE Symposium on Security and Privacy (S&P)*.

Appendix

1. Interview Guide

In the following, we present the interview questions used to conduct the semi-structured interviews.

Introductory Questions. The company and interviewee's role in it.

- Please describe in as much detail as possible your role within your company.
- How is the provision of hosting services embedded into the general business strategy of your company?

Technical Infrastructure Questions. General security posture of the company and identified risks.

- What are general security considerations that you deem relevant for the operation of your company's hosting services?
  - What are possible types of attacks ('threat models') affecting hosting services provided by your company?
  - What security-related risks are there for hosting services?
- What does your company exactly do to prevent this specific kind of attack / threat?
  - Are there specific departments in the company in charge of mitigating these risks?
  - Are there in-house developed tools, or external tools?

Legal obligations for maintenance.

- If possible, can you describe the legal regulations that the company has to abide to, concerning security maintenance of the hosting services?

Organizational Aspects Questions. Security management.

- How is management/handling of security events organized in your company?
- Does your company manage security events (when they happen) internally (by its own staff), or are they outsourced to an external contractor?
  - *If handled externally:* Can you please describe which type of company is this and what services they offer?
  - How are responsibilities distributed between your company (organization) and this external service provider?

- Is there any set of (internal) instructions on what to do in such situations (a "playbook" of some kind)?
- Are there specific people (organizational units) who are in charge of responding to security events?
  - Does addressing the report involve multiple teams?
  - Does the company distinguish between those who decide on remediation and those who implement it?
- Does addressing the report involve external stakeholders?

Personal security even handling experience.

- Did you ever experience any of these cybersecurity events at your company?
  - How did your company learn about the (security) event?
  - What was done in your company once the event was recognized?
  - What was your specific role in this process?
  - How did the whole situation end?
  - What would you describe as "lessons" that your company learned from this event?
- The course of action you described: Is it part of a procedure formalized by the company, or is it something informal?
- Is this procedure regularly followed?

Vulnerability Notifications Questions. Being informed about risks and events.

- How are vulnerabilities and other S&P problems detected in the infrastructure of your company's hosting services?
- Does your company have a dedicated channel for reporting vulnerabilities and other S&P problems?
- Does your organization receive vulnerability notifications from third parties?
- How does your company become aware of security events happening / happened?
  - *If no external source of info was mentioned:* Is there the possibility that the company would be informed of a security event from an external entity (person or organization) who were not contractors?

Vulnerability notification handling.

- *If they have received VN:* What did you do with the external report?
- *If they have never received a VN:* Imagine you've just received a report from an external describing a security issue on your servers.
- Please describe which factors played/would play into your evaluation when deciding on how to act on this message.
- Which challenges do you face when evaluating external security reports on security events?
  - How did/would the medium in which you received the report affect your decisions (e.g., email vs. contact form)?
  - How did/would the identity of the sender of the report affect your decisions?
  - What were/would be measures you applied/y to verify information in the report?
  - How did/would legal requirements influence your decisions?
  - How did/would your technical skills influence your decisions?
  - How did/would authority-related questions influence your decisions?
  - How did/would trust in the message in general affect your decisions?
- Can you please walk us through the steps you take/took to remediate a security report?
- Have you ever received security reports about systems that were not on your perimeter?

Vignettes describing specific VN issues.

- Malicious or suspicious behavior: a malware (e.g. `.exe`, or MS document with macro), a malicious file (e.g., a clickbait PDF), a file containing malicious code/functionality accessible from the web (e.g., a phishing page, a script redirecting to malicious/illegal content).
- Misconfiguration: a misconfiguration in HTTP headers enforcing security mechanisms (e.g. for transferring cookies), a misconfiguration in access control for a restricted area of a web app (e.g., default password, no access control).
- Code vulnerability: an error in the implementation of a software functionality, which can be observed via active testing or by passively observing indirect indicators (e.g., direct exploit of XSS, SQLi, or observation of software version indicators).
  - How would you say your company considers these vulnerabilities?
  - *If they are considered:* Which tools does your company use to keep track of these vulnerabilities?
  - *If they are considered:* Is there any regular maintenance task to prevent them?
  - *If they are considered:* When deciding whether to address a vulnerability, would it influence your decision to know that it is a malicious file / misconfiguration / code vulnerability?

2. Codebook

HPO.

- Business Aspects
  - Feel responsible for internet security
  - Ideologically driven hosting policies
- Business Considerations
- Services Offered
  - Maintenance
- Organizational Aspects
  - Company Structure
    - Communication Between Teams
    - Departments
  - The infrastructure-customer divide

- Functioning of Services
  - Take Action to Ensure SLA
  - Take Action to Safeguard Infrastructure Safety
  - Manuals
- CySec Aspects
  - Abuse of HPO Infrastructure
    - Our infrastructure does not care about phishing
  - Security Posture
    - General Proactive Measures
    - General Security Mindset
      - Keep updated
    - Incident Response
      - Proactive-Security Practices
      - Proactive-Security Software
      - Detection
      - Detection Software
      - Reactive-Security Practices
      - Reactive-Security Software
      - Incident Response
    - Organization Policies
    - Weaknesses
      - Customer Created
      - HPO Created
      - HPO-Customer Co-responsible
- External Relations
  - Externals Contacting HPO
    - Brand/ Phishing Protection Companies
    - Companies Reporting Phishing or Malware
  - Service Provider Relationship

Customer.

- Business model of your customer
- Characteristics
  - Customer Structure
  - Customer Tech-Savvyness
  - Customer Types
- Choice of Product / Service
- Customer Resources
  - Own IT Team
  - Own Software
- Mindset of HPO Customers
- Reaction to Security Event
- Relationship & Communication with HPO
  - Customer Complains to HPO
  - Customer Reports VN received
- Security Posture of Customer

Events.

- CySec Events
  - How
  - Detection Stage
  - Post-Incident Stage
  - Response Stage

Participant.

- Active Role
- Background / Professional Biography

Regulations.

- Certification
- Documents with Legal Implication
- Must-Dos
- Regulators
- Won't-Dos
- Legal Regulations for Security

Security Third Parties.

- CERT
- Google SafeBrowsing
- VirusTotal

Tech Used.

- Server-Side Software
- Tech for Hosting

Vulnerability Notifications.

- Assessment
  - Criteria
    - Business Criteria
    - Interaction-Based Verification
    - Validate Email Style
    - Validate Email Metadata
    - Validate Informative Content
  - Outcome
- Challenges
  - Customers Don't Understand
  - Unclear Motivations of Senders
  - Receive Spam
- Communication Channels
- Handling Method
  - Evaluation by Human
  - Gut Feeling or Experience
- Handling Practices
  - Validation via Sender Communication
- HPO's VN Knowledge
- Improvements
- Receiving Entity
  - Company Receives Notification
  - Customer Receives Notification
- Sender
- VN Exposure
- VN reachability

Others.

- Attack Types
- Information Sources

3. Meta-Review

The following meta-review was prepared by the program committee for the 2026 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

3.1. Summary. This paper presents a qualitative study of how 24 hosting providers manage vulnerability notifications, revealing that remediation efforts are shaped primarily by strict service boundaries, organizational structure, and the perceived responsibility for security issues, often resulting in limited action on reports. The findings highlight persistent gaps between the expectations of notification senders and real-world provider practices, emphasizing the need for clearer, more actionable recommendations for improving vulnerability remediation.

3.2. Scientific Contributions.

- Provides a Valuable Step Forward in an Established Field

3.3. Reasons for Acceptance.

1) Addresses a Key Gap: The work explores hosting providers' operational and organizational factors influencing vulnerability notification effectiveness, a perspective not previously examined in depth. This helps surface reasons for persistently low remediation not explained by notification-centric studies.
2) Diverse, Relevant Observations: Through semi-structured interviews with representatives of 24 providers of varying types, the authors collect a rich set of observations, enabling critical insights into policy, responsibility boundaries, and impediments to remediation.
3) Enables Further Research: The authors plan to release an original dataset of the studied services, supporting transparency and laying the groundwork for future research.

4. Noteworthy Concerns

1) Limited Scope Reduces Generalizability: The study is heavily weighted toward European organizations and excludes dedicated server providers, which may limit applicability of the findings outside the sampled segments.
2) Depth of Analysis and Actionability: The paper's stated recommendations may not be specific enough to be actionable for either hosting providers or reporters. Proposals for report standardization or improved communication would benefit from clearer, more concrete guidance rooted in the interview data.
3) Potential Respondent Biases: The study relies on participants' descriptions of their formal processes, which may differ from actual practices.