# Navigating the Patchwork: Investigating the Availability & Consistency of Security Advisories

Ronald E. Thompson III
*Tufts University*
Medford, MA, USA
rthomp06@cs.tufts.edu

Luke Boshar
*Tufts University*
Medford, MA, USA
luke.boshar@tufts.edu

Eugene Y. Vasserman
*Kansas State University*
Manhattan, KS, USA
eyv@ksu.edu

Daniel Votipka
*Tufts University*
Medford, MA, USA
dvotipka@cs.tufts.edu

***Abstract*—Prioritizing software patches requires accessible and consistent vulnerability information, but collecting this information through the current ecosystem of disparate organizations presents significant challenges for system administrators. This paper reports on the experience of systematically analyzing the security advisory practices of 718 organizations, including certified reporting bodies and vendors involved in critical infrastructure, detailing the hurdles faced in data collection and interpretation. Our findings show the disparities in public advisory availability across organization types and the lack of widespread usage of machine-readable formats, hindering automated processing. Additionally, while CVSS has been adopted across the ecosystem as the standard for severity scoring, in practice, its application suffers from inconsistencies in reporting completeness, versioning, and transparency, limiting practical utility for system administrators and researchers to perform comparisons. This work provides an empirical baseline of the advisory ecosystem, highlighting the practical barriers encountered, and underscores the need for improved reporting consistency, transparency, and active coordination to support practitioners and researchers.**

***Index Terms*—Security Advisories, CVSS, Vulnerability Management**

## I. Introduction

Keeping software up-to-date by patching identified security vulnerabilities is a critical challenge in modern software ecosystems [52]. Patching a production system can be complex, as it might require service downtime and could further disrupt operations if the patch is incompatible with other integrated software and systems. Compounding this problem, system administrators (sysadmins) often can be faced with needing to patch many vulnerable systems in their network after running a vulnerability scanner [5] or proactively searching for software updates [18], [35]. This means sysadmins must triage patches, prioritizing based on various factors, including vulnerability severity, criticality of affected systems, and potential for disrupting operations [5], [18], [24], [30], [35], [52].

To make these assessments, many sysadmins rely on security advisories that contain pertinent information to evaluate a patch and the associated vulnerabilities [18], [35]. Various organizations publish these advisories, including software vendors, government organizations, and security vendors. We refer to these groups collectively as stakeholders. Security advisories often include a vulnerability severity assessment and recommended mitigation strategy. The severity assessments typically use the Common Vulnerability Scoring System (CVSS) [9], [15], [38], [50]. CVSS is a metric developed and maintained by the Forum of Incident Response and Security Teams (FIRST) to evaluate the severity of vulnerability by rating it across several features, assessing the ease and technical means of exploitation and impact if exploited, and finally producing a value between zero and ten [20], [38].

Prior work has shown sysadmins struggle to process all relevant information from these advisories, including determining which stakeholders' advisories are likely to be reliable [18], [24], [30], [35], [54]. Additionally, research has shown some stakeholders can be inconsistent in what information they present, focused almost exclusively on the US National Vulnerability Database (NVD) [2], [4], [19], [22], [29], [31]–[33], [40], [58], further complicating sysadmins' jobs.

While these studies highlight specific inconsistencies and sysadmin challenges, a broader understanding of the advisory ecosystem is lacking. A complete picture of the ecosystem is necessary to grasp the sysadmins' experience when seeking information about new vulnerabilities. Furthermore, taking a comprehensive snapshot of the ecosystem is crucial for researchers examining the quality of available data. We set out to investigate security advisory availability and consistency across a broad and diverse 718-stakeholder sample by attempting to build a corpus of their security advisories. This paper reports on our experience undertaking this effort. We detail the practical challenges encountered during this effort, including data discovery, accessibility, formatting, and consistency. Our primary contribution is sharing this experience, providing an empirical baseline characterization of the advisory ecosystem derived directly from the practical hurdles of data collection, and offering lessons learned and recommendations grounded in this real-world data collection.

Our attempt to characterize the ecosystem and understand the associated challenges was guided by the following specific research questions:

**RQ1** How available and accessible are security advisories?
**RQ2** How often are these presented in a structured, easily machine-processible format?
**RQ3** How consistently do advisories report CVSS information for vulnerabilities in their advisories?

Due to the vast number of potential software vendors who could produce security advisories, we focused our study on two groups of stakeholders. The first were stakeholders certified by MITRE as CVE Numbering Authorities (CNAs). CNAs serve as exemplars because they must meet requirements related to coordinated vulnerability disclosure and have established security groups within their organizations. We also included vendors mentioned in CISA's Industrial Control System Advisories (ICSAs). Due to the proliferation of vulnerabilities within and the highly regulated nature of industrial controls [9], [15], [48], [50], stakeholders associated with these ICSAs operate under increased scrutiny and regulatory requirements, making them more likely to have available security advisories.

Our analysis focused on public advisories, reflecting CNA requirements [14], operator search behavior [18], [30], [35], and the baseline for automated tools. While non-public channels undoubtedly exist and are used, understanding this public landscape is a critical first step. We examined the use of structured data formats (e.g., CSAF [49], JSON) to assess feasibility for automated collection. This is a known operator requirement [5], [18], [35] and also crucial for large-scale research review. Finally, we focus on CVSS data as it is a commonly used [36], [43], [53], [57] and recommended metric [9], [15], [38], [50] that provides a structured way for sysadmins to compare the perceived severity of a vulnerability across different stakeholders.

In our analysis of 718 unique CNA and ICSA stakeholders, we found significant disparities in the public availability and format of security advisories. While nearly all CNAs (94.7%) provided public advisories as expected, fewer than half of ICSA vendors (38.4%) did so. Further, these advisories were often challenging to find, requiring significant manual effort to search through stakeholders' websites. Among the 460 stakeholders with public advisories, the vast majority (93.3%) used inconsistently formatted (i.e., the same information is not included in every advisory) web pages or PDFs, with only 30 offering structured, machine-readable data. Furthermore, just over half included any form of severity assessment (63.7%).

On a positive note, when severity assessments were provided, the vast majority utilized the same predominant method, CVSS (82.6%) and major version (i.e., v3.x; 75.6%), and most of those provided both the CVSS score and vector, indicating some details of the assessment (86.4% of stakeholders using CVSS). Unfortunately, stakeholders were inconsistent when providing further context necessary for sysadmins to apply these assessments to their own environments or for researchers comparing scores across the ecosystem. This includes using a mix of CVSS versions or not clearly stating the version (23.2% of stakeholders using CVSS), not using temporal (83.9% of stakeholders using CVSS) or environmental (95% of stakeholders using CVSS) metrics, not providing clear rationales for assessment decisions, and only providing assessments per-vulnerability (69.4% of stakeholders using CVSS), rather than also including an aggregate score for the advisory, which often covers multiple vulnerabilities fixed by single patch.

Our findings highlight considerable friction in the public advisory ecosystem, which makes it difficult for sysadmins and researchers to collect and compare information. Our work overcomes some of these hurdles to produce a listing[1] of CNAs and ICSA vendors who provide public advisories, along with links to their advisories to support sysadmins and researchers' searches. We also offer recommendations based on our results for sysadmins and future researchers seeking to collect and analyze security advisories.

## II. Related Work

We now discuss our work in the context of prior work that looks at the information used by sysadmins for vulnerability assessment and triage, as well as prior security advisory reviews.

**The information sysadmins use for triage.** There has been an increasing amount of research into how sysadmins make decisions around patching and triaging vulnerabilities that affect their systems, specifically looking at how sysadmins decide when and what to patch [18], [30], [35], [54]. For example, Li et al. found sysadmins reported making patching decisions based on the vulnerability's severity, with the highest emphasis on critical vulnerabilities [35]. In a survey of sysadmins, Jenkins et al. found that while some conduct risk assessments themselves to determine the severity of impact a vulnerability could have on their own systems, this was uncommon due to the high overhead of performing this assessment and lack of expertise, instead relying on publicly reported severity assessments [30]. Unfortunately, this prior work and other studies have found sysadmins report finding it difficult to find comprehensive information about all the vulnerabilities they are impacted by from public advisories [18], [30], [35]. In our work, we seek to quantify this challenge by investigating what severity information is available across the security advisory ecosystem and assessing how difficult it is to navigate this landscape.

**Sources of vulnerability information.** Other researchers have compared differences in the information presented in security advisories between vulnerabilities [2], [4], [19], [22], [31]–[33], [40], [42], [58]. Almost all of these have only considered advisories found in the NVD, with only two considering multiple stakeholders. Specifically, Forain et al. compared the NVD to China's vulnerability database [22] and Moriuchi and Ladd performed a similar comparison with Russia's vulnerability database [42]. Additionally, this prior work has focused on discrete parts of security advisories. This includes the products and versions affected by vulnerabilities [2], [19], [31], [33], estimating vulnerability severity [2], [33], the relationship between severity and patching [3], [40], [43], severity and exploit existence [4], [29], and the difference in information observedstakeholders [23], [40]. For example, Anwar et al. conducted a comprehensive evaluation of the NVD, examining issues related to data completeness and inconsistencies in publication dates and product names [2]. In the NVD, advisories

[1] The full listing of stakeholders and their information can be found in our supplementary materials at https://osf.io/vfch3/?view_only=20ae77e8d964468faa42281c73921905

list affected products using a standardized string format to uniquely identify classes of hardware, operating systems, and software applications. Unfortunately, they found that these strings were inconsistently provided and applied, which can lead to issues in identifying whether a system is vulnerable during automated scanning. We observed the same problem among some of our data and discuss this in Section III-A. Miranda et al. analysed all the pages referenced by the NVD to see when information was published by different stakeholders [40], focusing on the timing of information. Zhang et al. focused on the discrepancies of similar vulnerabilities within the NVD [58]. Compared to these studies, our work provides a broader characterization of the landscape of stakeholders' vulnerability data, specifically how this information is presented, such as formatting and availability issues. We focus on the advisory publication practices of stakeholders rather than specific inconsistencies in a single data set as in prior work. Thus, we enable larger-scale studies expanding on this prior work to capture the full range of available security advisories.

## III. Methodology

We now discuss how we reviewed and assessed security advisory availability, accessibility, and consistency. We begin by describing the stakeholders included in our dataset, then describe how we found and reviewed their security advisories. We conclude by discussing the limitations of our process.

### A. *Security Advisory Stakeholder Selection*

To begin, we first had to identify stakeholders who produce security advisories for vulnerabilities. To identify organizations we expected would produce these advisories, we considered two sources: advisories regarding Industrial Control Systems (ICS) and medical devices published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), as well as MITRE's registry of CVE Numbering Authorities (CNA). We describe each, why they are relevant, and discuss how we identified stakeholders from these sources in turn below. We provide a list of all the stakeholders we evaluated in our supplement materials [1]. We identified 393 stakeholders from the CISA ICS advisories and 379 stakeholders in the MITRE CNA registry, with 718 unique stakeholders total (54 stakeholders were in both groups).

**CISA ICSA vendors (393 stakeholders).** CISA coordinates cybersecurity programs within the U.S. Government, including sharing and coordinating information on vulnerabilities affecting ICS and medical devices [11], [27], [28]. As part of this mandate, CISA provides the public with information about specific vulnerabilities affecting these devices in the form of ICS Advisories and ICS Medical Advisories (collectively referred to as *ICSAs*) [16]. Because ICS and medical devices are used in highly regulated industries, such as nuclear energy and healthcare, they are subject to regulations about vulnerability disclosure and remediation [9], [15], [48], [50]. Therefore, we included the vendors mentioned in ICSAs as stakeholders targeted during our data collection as we expected they would have publicly available vulnerability severity information and would offer an upper bound approximation for security advisory availability, accessibility, and consistency.

To find the vendors associated with these advisories, we reviewed all 2,112 ICSAs from the time CISA began publishing them, i.e., July 2017, until March 6th, 2024—the date we performed this collection. For each ICSA, we extracted all the listed vendors, which we refer to as ICSA vendors going forward. Because some ICSAs include multiple related vulnerabilities, many mention multiple vendors. For example, ICSA-19-106-03, which included the ICSA vendor string "ABB, Phoenix Contact, Schneider Electric, Siemens, and WAGO," indicating five unique ICSA vendors. We identified 393 unique ICSA vendors in the 2,112 ICSAs.

**CNAs (379 stakeholders).** The MITRE Corporation maintains a list of stakeholders certified as CNAs listed on cve.org. To be certified, a CNA must maintain a public source for new vulnerability disclosures [14]. This can include ICSA vendors and third-party security organizations who provide information about vulnerabilities (e.g., Cisco Talos). Due to the requirements, all CNAs should have public advisories and have demonstrated an ability to assess vulnerabilities. We also collected the list of CNAs on March 6th, 2024, and found 379 unique CNAs.

**Identifying unique stakeholders.** After collecting the list of CNA-certified and ICSA-mentioned stakeholders, we needed another post-processing step. As organizations frequently change ownership, this may sometimes result in changes to who manages their security advisories, requiring a careful review of new digital assets. For example, some organizations have been acquired, and their digital presence has been consolidated with the acquirer. One example is St. Jude Medical, acquired by Abbott Laboratories in 2017. In other cases, the organizations still maintain their prior digital presence and CNA status as independent organizations, such as Hitachi, which is associated with three CNAs, two of which are also ICSA vendors. The third type of change can occur when organizations are split up. For example, General Electric has evolved into three distinct entities: GE Aerospace, GE Healthcare, and GE Vervona. In these cases, we manually mapped the CNAs/ICSAs to the new organizations by examining the mentioned products and their associated divisions.

Two researchers who reviewed each stakeholder performed this process by first identifying their website. For ICSA vendors, they checked if the ICSAs mentioning the ICSA vendor contained links to the ICSA vendor's website. If there were no links, the researcher performed a Google keyword search for the ICSA vendor's name and the specific product(s) mentioned. The CNA list contained links to the CNA's advisories directly, which provided researchers with a direct link to the organization's website. However, these links did not work in some cases, and the researchers used the same keyword search as they had for the ICSA vendors. Once a website was identified, we checked if a parent organization was associated with the stakeholder. They did this by seeing if there was a redirect on the organization's website, checking the

Corporate Information and Terms of Service listed on the site for any mention of a different organization, and looking up the organization on Bloomberg [7], Wikipedia [56], and Crunchbase [12]—three well-established repositories of organization information [6], [34]. After identifying the organization-to-parent mapping, if we could not find security advisories for the organization, we then looked to see if the parent maintained any advisories for our analysis.

### *B. Advisory Review*

After identifying the stakeholders, we wanted to understand what information they provide publicly about vulnerabilities. Public vulnerability disclosure information is vital to sysadmins, who then use it to determine their best triage actions, and researchers who use it to investigate trends in vulnerability reporting. As discussed in Section III-A, CNAs must make this information public; however, it is unclear whether MITRE enforces this requirement and how easily the data can be accessed. Here, we describe the vulnerability information we collected from each stakeholder and the process we followed.

**Advisory identification.** Our first step to assess security advisory availability was to identify whether each of the stakeholders provided security advisories. For this analysis, we loosely define advisories as assessments of one or more vulnerabilities; that is, they can include individual vulnerabilities. This could include detailed descriptions of vulnerabilities or a dashboard with minimal vulnerability and severity information. To identify relevant advisories for each stakeholder, two researchers performed a Google website search, i.e., using the search tag "`site:`", with the website identified during the unique stakeholder check. For each stakeholder website, we conducted queries for the following keywords: `psirt` (i.e., Product Security Incident Response Team), `product security`, `security advisory`, `security bulletin`, `cybersecurity`, and `cve`. Some CNAs had direct links to their advisories in the MITRE list, which were used when possible. For each site, we noted any mention of security advisories or vulnerabilities.

**Advisory assessment.** If we could identify advisories, the researchers then checked whether they could access them. Was the data publicly available, or was account registration necessary? Were there limits on who could register (e.g., customers only) if registration was required? For stakeholders with public advisories, the two researchers made the following determinations about the advisories:

- **Are advisories posted in a structured data format?** Were the advisories published in a format that could be automatically processed, such as JSON or CSAF (a vulnerability advisory specific format [49])? This is a critical step in supporting sysadmins' automated vulnerability triage [18], [35] and advisory-based research.
- **Do advisories provide a vulnerability assessment?** Regardless of the methodology used, did the stakeholders provide some sort of assessment about the vulnerability that sysadmins can use for prioritization?
- **Do all or some advisories provide a per-advisory and/or per-vulnerability assessment?** If advisories only contained single vulnerabilities, then this was treated as only per-vulnerability and not per-advisory. Per-vulnerability assessments offer a standardized measure of individual flaw severity, enabling comparison between distinct issues and across sources. Per-advisory assessments are needed for operators to gauge the overall severity and priority of security patches that address multiple vulnerabilities simultaneously.
- **If CVSS is used, are the score and vector provided?** The vector is critical as it gives a detailed breakdown of the stakeholder's severity assessment. Additionally, we evaluated whether these CVSS values were reported at both the per-advisory and per-vulnerability levels. We also noted if this CVSS information was given for all advisories or only some (i.e., at least one advisory).
- **If CVSS is used, which CVSS version(s)?** CVSS now uses three distinct versions, each with a different structure, limiting comparisons [2], [31], [33]. Given that assessments done using different versions cannot readily be compared, it is important for sysadmins's to know what version was used [46], [47]. We also noted if the versions used were consistent (i.e., all advisories used version 3.1) for all advisories.
- **If CVSS is used, are Environmental/Temporal features added?** CVSS uses environmental and temporal components to account for specific vulnerability contexts [25], [26]. These metrics are valuable because they refine prioritization by adding crucial context about the current threat landscape (e.g., exploit availability) and specific organizational impact to the static base vulnerability score [25]. As with the other CVSS-related information, we noted if this was provided for every assessment or if it was limited to only some.
- **Do the advisories use a qualitative label for the vulnerability?** We noted if the stakeholder provided a qualitative assessment for the label, such as *Critical, High, Medium, Low*, either in addition to or instead of CVSS. We then determined if that qualitative system relied on an industry standard, such as the NIST scale corresponding to CVSS scores [45], or if it was unique to the stakeholder. Qualitative severity labels (like Critical or High) allow sysadmins to quickly categorize vulnerabilities into broad groups, facilitating faster initial triage and prioritization decisions.

### *C. Limitations*

While this process allowed us to capture a large dataset of advisories, our analysis has limitations that provide context for the results.

First, our sample does not capture all possible vulnerability disclosure stakeholders. We intentionally focused on two groups: CNAs and vendors mentioned in ICSAs. CNAs serve as exemplars, representing organizations that have undergone a certification process and invested effort in establishing pub-

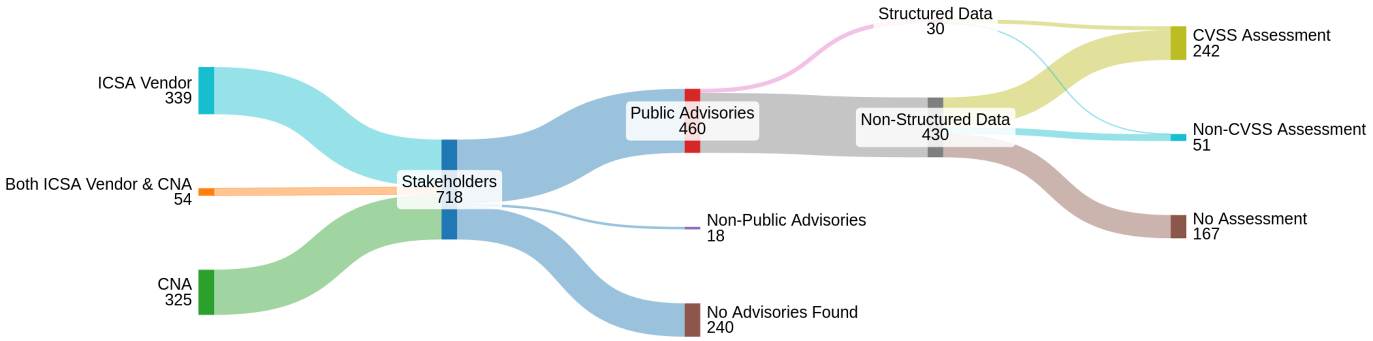

Fig. 1: The data available in advisories from the 718 stakeholders that we evaluated.

lic vulnerability disclosure procedures [14]. Including ICSA vendors provides insight into practices in higher-scrutiny sectors [9], [15], [48], [50], although this subset does not represent all ICS vendors globally. Consequently, while our findings provide valuable insights into these large and relevant groups, the specific practices observed may not fully generalize to the entire universe of software producers, particularly smaller organizations or independent researchers not included in these lists, and should be considered an upper bound.

Secondly, despite efforts to ensure consistency, manual data extraction from diverse, inconsistently formatted sources can potentially introduce interpretation errors. To mitigate this, two researchers reviewed each stakeholder iteratively, refining classifications for advisory availability, format, and reported CVSS components (version, vector, score, supplemental metrics). Crucially, our assessment scope was intentionally limited to objective, verifiable data points explicitly reported in advisories (e.g., presence of a score, stated version, use of a structured format). We did not perform a subjective analysis of advisory content (e.g., assessing the quality of mitigation advice); instead, we focused on characterizing the reported structures and data presence at scale. This aligns with our goal of providing a broad baseline but limits insights into content quality. Therefore, our choice not to perform qualitative coding or calculate inter-rater reliability is appropriate according to best practice [37]. This focus enhances reproducibility for the specific data points collected. In cases where there was disagreement or ambiguity, the two researchers discussed these conflicts and refined their strategy to reflect any clarifications.

Finally, our study faces discovery limitations. Our analysis primarily characterizes publicly discoverable advisories accessible via website navigation and search engine indexing. We acknowledge that some stakeholders restrict access via customer portals ($N = 18$ confirmed, potentially more undetected), and advisories not well-indexed by search engines or hosted in obscure locations might have been missed. Therefore, our findings regarding the prevalence of public advisories and specific reporting practices represent the baseline accessible landscape but likely underestimate the total volume of advisories produced, particularly those shared through non-public or restricted channels. However, understanding this publicly accessible baseline remains crucial, as it reflects the information most readily available to sysadmins during proactive searches [18], [30], [35] and forms the foundation for developing broadly applicable automated tooling.

### D. *Ethics*

All data analyzed in this study were collected from publicly accessible sources, whether organizational websites or public repositories. Our analysis focuses exclusively on the public disclosure practices of organizations and the format of the advisories they produce. The research did not involve human subjects, private data, or any form of interaction that would necessitate Institutional Review Board (IRB) approval.

## IV. Results

Our analysis incorporated 718 unique stakeholders involved in vulnerability disclosure, identified through CISA's ICSAs and the official CNA list. This set includes 339 stakeholders who were only ICSA vendors, 325 who were only CNAs, and 54 who were both. Four organizations listed as ICSA vendors lacked any discernible web presence and were thus categorized as having no public advisories available. Below, we outline our findings regarding the availability and consistency of advisory data.

### A. *Advisory Availability (RQ1)*

The accessibility of public security advisories varied significantly between CNAs and ICSA vendors. Figure 1 provides a Sankey diagram that visualizes the breakdown of stakeholders by advisory availability and format.

**Non-CNA stakeholders were unlikely to make advisories public.** As anticipated due to CNA requirements, nearly all CNA stakeholders (including those also listed as ICSA vendors) provided public advisories (94.7%, $N = 359$). However, ICSA vendors who were not also CNAs were much less likely to make their advisories publicly available (29.8%, $N = 101$). When considering all stakeholders mentioned in ICSAs (both CNA and non-CNA), fewer than half (38.4%, $N = 151$) had public advisories. Notably, a third of these publicly available ICSA vendor advisories came from organizations that were also CNAs ($N = 50$).

**Security advisories can be hard to find.** Even when stakeholders made their advisories public, it often took us some time to find these advisories. While some large organizations maintained dedicated, easily identifiable product security pages (e.g., Cisco, Palo Alto Networks), many others integrated advisories into less obvious locations, such as general blogs, news sections, or knowledge bases (e.g., Synopsys, Progress Software). Further, many of these stakeholders without dedicated advisory pages lacked effective search or filtering capabilities specifically for security advisories, potentially hindering the ability of sysadmins to locate relevant vulnerability information efficiently. We could only find the advisories for these stakeholders after searching several keywords and manually reviewing long lists of returned and often irrelevant pages. This demonstrates the effort potentially required by sysadmins seeking this information proactively.

### *B. Machine Readable Advisories (RQ2)*

Considering the stakeholders with publicly available advisories, we now focus on how this information is presented. First, we discuss whether the advisories were machine-readable, necessary for large-scale collection and analysis by sysadmins and researchers. Despite the recognized need for automation in vulnerability management, the adoption of structured, machine-readable formats for advisories was minimal. The fourth column of Figure 1 summarizes our results for this section.

**Few stakeholders adopted standardized structures.** Only 30 stakeholders (6.5% of stakeholders with public advisories) provided advisories in a structured, machine-readable format. The formats observed included CSAF ($N = 15$), CVE JSON [41] ($N = 8$), and others ($N = 7$). This low adoption rate significantly hampers sysadmins' and researchers' efforts to automate the ingestion and processing of vulnerability information across the ecosystem.

**Unstructured formats were most common.** The overwhelming majority of stakeholders with public advisories relied exclusively on unstructured formats (93.3%, $N = 430$). This primarily included HTML web pages or PDF documents that did not follow any standardized structure, and where relevant fields were not clearly tagged. Parsing these pages and documents would require significant effort to write custom parsers. Further, the formatting within these unstructured advisories often varied significantly, not only between different stakeholders, but sometimes even within the advisories published by a single stakeholder over time. For example, ABB provided advisories in PDF form, but changed their format over time due to mergers and the general evolution of their template. The location of the vulnerability details changed in these different formats, as did the headline that an sysadmin might search for. This inconsistency means anyone attempting to parse these PDFs at scale would have to formulate a new process or manually write a new parser for each change, significantly increasing data collection overhead.

### *C. CVSS Consistency (RQ3)*

Finally, for each of the stakeholders with public advisories, we looked at whether and how they reported vulnerability severity assessments, the primary information sysadmins need when assessing a new vulnerability. The furthest-right column of Figure 1 summarizes our results in this section. We specifically focus on the use of CVSS, as it provides a standardized approach to severity assessment. However, while CVSS provides a general standard, we found its application in public advisories is inconsistently applied between stakeholders. We observed variation in whether it was available, whether stakeholders provided complete information from the assessment, and what version of the CVSS score was used. Figure 2 details the specifics of CVSS assessment practices among the stakeholders who utilize CVSS.

**Only a slight majority of stakeholders provided severity assessments; mostly using CVSS.** Among the 460 stakeholders with public advisories, only 63.7% ($N = 293$) included any form of severity assessment. This was surprising as prior work has found this is one of the most important questions sysadmins have when investigating a new vulnerability [18], [35]. When severity assessments are provided, CVSS was by far the most common method (82.6%, $N = 242$). The other stakeholders utilized unique quantitative or qualitative scales ($N = 51$). For example, SAP rated vulnerabilities as "Hot News", "High", "Medium", or "Low". Unfortunately, few of these stakeholders indicated what qualified a vulnerability to fall into each of these categories, so it very difficult to compare severity assessments between stakeholders beyond the extreme ends of each scale.

**Most advisories using CVSS included the score and vector.** Within the 242 stakeholders using CVSS, there was considerable variation in how CVSS components were reported. However, one positive finding was that almost all stakeholders—for at least one advisory—provided a CVSS score (99.2%, $N = 240$), the vast majority provided the vector string (87.2%, $N = 211$), and most provided both (86.4%, $N = 209$). Only a few stakeholders provided just the CVSS score without the accompanying vector (12.8%, $N = 31$) and a negligible number provided only the vector (0.8%, $N = 2$). This is beneficial because there are many instances where two vectors (i.e., assessed vulnerability characteristics) can yield the same CVSS score. In these cases, it would be impossible for an sysadmin or researcher to determine the difference between the two vulnerabilities and the differential impacts they might have in different environments. Considering all possible CVSS v3.1 vectors (i.e., all possible combinations of the base metrics), 98.8% had another vector with the same CVSS score.

**Some stakeholders are inconsistent or unclear about the CVSS version used.** Due to the scoring and vector changes between major CVSS versions (e.g., v2.x to v3.x), it is difficult to compare scores between versions. On another positive note, most of the 242 stakeholders using CVSS used v3.x, i.e., v3.0 or v3.1 (75.6%, $N = 183$). Only a small fraction still referenced v2.0 (1.2%, $N = 3$). However, a notable group

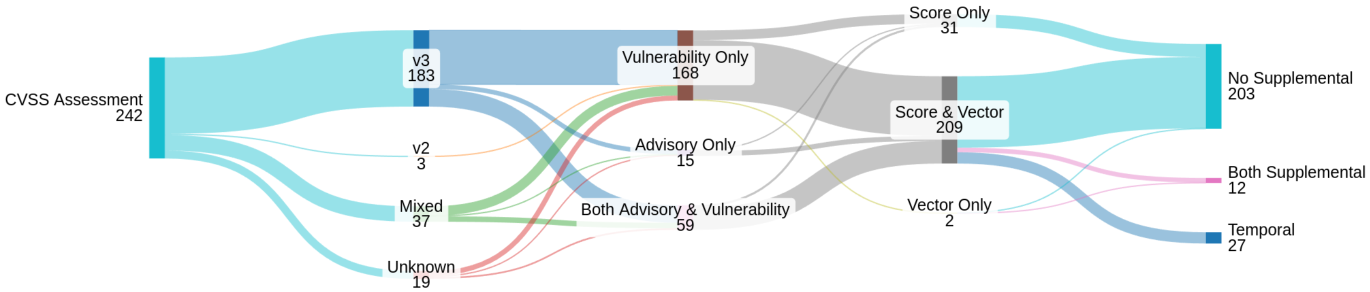

Fig. 2: The data available in advisories from the 242 stakeholders with public advisories (from Fig 1).

used a mix of versions between advisories (15.3%, $N = 37$), i.e., they used one version for some advisories and then a different version for others, and 7.9% ($N = 19$) did not specify the version used, although this can be mitigated in part by providing the vector. Furthermore, we note that the consistency in use of v3.x may currently be in flux as FIRST recently released v4.x, and since our data collection, we have begun to see its adoption anecdotally.

**Few stakeholders used supplemental metrics; fewer applied them consistently across advisories.** CVSS temporal and environmental metrics, designed to provide context-specific adjustments, were rarely used. Only 16.1% ($N = 39$) of stakeholders using CVSS incorporated any supplemental metrics. Of these, most used only Temporal metrics ($N = 27$), none used only Environmental metrics ($N = 0$), and a few used both ($N = 12$). Furthermore, usage was often inconsistent; 87.2% ($N = 34$) of stakeholders using supplemental metrics applied them only in some advisories rather than uniformly.

**The majority of stakeholders assess vulnerabilities individually.** We found the majority of stakeholders only provided CVSS assessments for vulnerabilities individually ($N = 168$, 69.4% of stakeholders that provided public CVSS assessments). Because security patches can fix multiple vulnerabilities, this forces sysadmins to determine an aggregate severity for all the vulnerabilities fixed by the patch to determine the patch's total impact. Aggregating vulnerability severity scores is challenging as sysadmins, who may not have time to complete extensive testing, would not understand how the vulnerabilities might interact like a vendor who publishes the patch and advisory might. Therefore, providing both advisory-level and individual-level severity scores can be valuable.

It is also valuable for sysadmins and researchers to know how vulnerabilities are aggregated to create an advisory-level score. Considering stakeholders who provided both a vulnerability- and advisory-level assessment ($N = 59$, 24.4%), we observed that all stakeholders applied the highest (i.e., most severe) individual vulnerability CVSS score as the advisory-level score. We expect this trend to continue for the 15 other stakeholders who only provided advisory-level assessments as their advisory-level scores matched the most severe individual-level score given by another stakeholder. However, other score aggregation processes may be used.

**Few stakeholders give scoring rationale or provenance.** Beyond the quantitative reporting of CVSS components, we observed a general lack of qualitative explanation regarding assessment decisions and indications of whether the assessments were their own or copied from others (i.e., data provenance). Understanding why a particular score was assigned is crucial for sysadmins attempting to contextualize the risk within their specific environment. For example, CVE-2023-20267—a vulnerability in Cisco's threat defense software, Snort—was rated more severe by the NVD than Cisco itself because the NVD rated the Attack Complexity as High, while Cisco rated it Low. After review by the Cisco security team, it was determined that this discrepancy was due to the vagueness in Cisco's description of the vulnerability and lack of direct reasoning for the score [39]. The vulnerability description only mentioned the need to spoof an IP address to trigger the vulnerability, which would be relatively simple, hence the Low for Attack Complexity from the NVD, which only had this description to work from. However, after internal review, the security team determined the spoofed IP address would need to be a specific address, which would be very challenging to mimic without detection. This confusion could have been avoided if Cisco had included this additional detail as reasoning for its CVSS assessment. Unfortunately, these justifications are uncommon among stakeholders, likely leading to more of these types of confusions. An exception was Becton Dickinson (BD), which provided clear rationale sections in their advisories for both first-party software vulnerabilities and third-party component vulnerabilities, explaining the reasoning behind their CVSS assessments. Other stakeholders, such as Siemens, included some vulnerability information, but not with the same clarity and detail as BD.

Furthermore, it was often unclear whether a reported CVSS assessment represented the stakeholder's independent analysis or was copied from another source like the NVD, complicating efforts to trace assessment origins or perform comparisons of assessments across stakeholders as some researchers have attempted [22], [42]. This general lack of transparency in rationale and provenance presents a significant challenge for interpreting and comparing CVSS scores effectively.

## V. Discussion and Recommendations

Our experience demonstrates the challenge of consistently capturing a complete picture of vulnerability severity across the security advisory ecosystem. Even for stakeholders managing some of the most sensitive systems, i.e., ICSA vendors, who have government oversight and support, most do not provide public security advisories, or their advisories are hard to find. While the security advisories are more available for CNAs, who are required to have public security advisories, they are still challenging to find and the vast majority of all stakeholders' security advisories are difficult to access at scale due to the very inconsistent use of structured machine-readable formats. These availability and accessibility issues present problems for sysadmins and researchers seeking ot collect this information. Even when the data is public, significant manual effort is necessary for each stakeholder to find their security advisories, identify relevant elements, and generate custom parsers—sometimes multiple per stakeholders—to collect relevant information.

Our dataset listing stakeholders with public advisories, along with links to their advisories [1], partially solves the first challenge of finding the advisories. This may be sufficient for sysadmins who work with a limited set of vendors and can manually review advisories as new vulnerabilities are identified. However, we expect this will only work for a small number of sysadmins as many have reported needing automation to keep up with the volume of vulnerabilities in real-world networks [18] and the links or stakeholder coverage will likely only be temporarily sufficient as companies change, e.g., going out of business, merging, or new vendors join the market. Therefore, to support sysadmins long-term and researchers in all cases, our experience demonstrates that significant effort will be necessary to write custom parsers for each new or updated stakeholder to enable large-scale collection. In addition, these parsers will need to be updated as we observed variations within stakeholders.

These problems become even more challenging when considering the specific information provided. Even when security advisories are publicly available and after custom parsers are written to capture relevant data, we observed inconsistencies in the provided severity assessments, creating practical challenges to their interpretation and comparison. While CVSS appears to have standard adoption when severity assessments are available, and both scores and vectors are generally provided, severity assessments were only supplied in a slight majority of cases. Comparability is complicated by version fragmentation across advisories (mixing v2.0, v3.x, or using unspecified versions) and the rare ($N = 39$) and inconsistent use of supplemental temporal/environmental metrics, preventing reliable severity comparisons over time or between stakeholders. Additionally, the predominant focus on individual CVE assessments (69.4%), frequently without nuanced advisory-level scores beyond simply adopting the maximum individual score, limits utility for sysadmins assessing cumulative patch risk. Finally, the frequent lack of transparency regarding why a specific score was assigned and who performed the assessment hinders the trustworthiness and deep interpretation of reported severities, concerns that sysadmins have raised in prior work [18], [35]. These issues present more fundamental challenges for sysadmins and researchers, even at the lowest scale of analysis. Without clear and consistent application of CVSS assessments, it is not possible to make robust comparisons of assessments across stakeholders.

Our experience reveals an ecosystem made up of a patchwork of stakeholders each making their own decisions about the presentation and application of security advisories. This creates a challenging ecosystem, and in parts, impossible to navigate, interpret, and compare. Therefore, our work provides quantitative evidence indicating why sysadmins in prior work regularly point to challenges in navigating this ecosystem as a primary challenge in their patching process [18], [35].

### A. Recommendations for Researchers & Stakeholders

Based on our results, we now discuss the implications for research on measuring the characteristics of security advisories. Additionally, replicating our level of effort as the ecosystem evolves, along with the extra work required to collect data from most security advisories, is unsustainable in practice. We provide recommendations for stakeholders and regulatory bodies based on our results to minimize collection costs and improve the value of this data.

**Recommendations for future research.** Our experience demonstrated the level of effort necessary to thoroughly capture security advisories across stakeholders, as well as several potential pitfalls which could impact the reliability of research results. First, we outline a thorough method for identifying stakeholders and finding their security advisories, then outline the challenge of capturing security advisory data at scale as easily machine-readable formats are not often used. Researchers should plan to allocate considerable resources for discovering and collecting public advisories. If researchers only rely on stakeholders with structured data, they will most likely have an unrepresentative sample.

Additionally, due to the inconsistency across stakeholders, researchers must spend time in data validation and cleaning to avoid likely errors due to the complexity of the underlying data. Further, the data will need to be carefully standardized to account for variations in CVSS version, advisory- versus individual-level of severity assessment, and the use of supplemental metrics. Additionally, researchers should strive to use data only from stakeholders who provide CVSS vectors, enabling them to understand the values chosen for that score and to infer the CVSS version if it is not provided. Without these specifics to add context, this vagueness introduces potential confounding factors that could impact any analysis.

**Need for active vulnerability coordination authorities.** Our findings highlight a significant challenge in advisory availability: while established CNAs largely provide public advisories (94.7%, $N = 359$), many other stakeholders, such as non-CNA ICSA vendors (29.8%, $N = 101$), do not consistently share this crucial information. The vulnerability disclosure ecosystem is currently in a dynamic state of transition, evidenced by the emergence of new national and regional databases like the EUVDB [21], initiatives such as the CVE Foundation [13], and ongoing challenges with established repositories like the NVD [44], [51], [55] and MITRE CVE program [8]. This period of change presents a crucial opportunity to develop an improved and more consistent system for disseminating vulnerability information. Merely providing passive data repositories appears insufficient. There is a critical need for active coordination authorities to assist organizations, particularly those with limited resources (such as many ICSA vendors), in establishing effective public disclosure programs and promoting standardized practices, including the use of structured data formats, thereby enhancing the overall information landscape.

Exemplary active coordination efforts, such as CISA's Coordinated Vulnerability Disclosure program [17] and CERT@VDE's work in the European industrial automation sector [10], serve as valuable models and strong starting points. CISA's provision of machine-readable CSAF data for its ICSAs is commendable; further enhancing the consistency and comprehensiveness of such structured data across all its advisory outputs would significantly increase overall utility. Similarly, CERT@VDE offers consistent and valuable support through its HTML-based advisories, and supplementing these with standardized machine-readable formats, such as CSAF or JSON, would significantly improve their accessibility for automated tools and broader data aggregation efforts. Supporting and expanding these and similar active coordination functions, with a dual focus on increasing both the raw availability of advisories and the adoption of standardized machine-readable formats, is essential for improving the overall vulnerability information landscape.

**Enhancing transparency with CVSS scoring rationale.** Beyond the scores themselves, understanding the justification for CVSS assessments proved challenging; our analysis found limited transparency in how stakeholders arrive at specific metric values. This aligns with broader industry observations, such as those presented by Cisco regarding discrepancies stemming from limited information or interpretation differences [39]. To improve the utility and trustworthiness of CVSS scores, stakeholders should provide justifications for their metric choices, creating a more transparent assessment. Detailing the reasoning, particularly for metrics influencing Attack Complexity or Scope as suggested in industry best practices, would allow sysadmins to contextualize scores better and make more informed decisions.

**Establish practices for advisory-level assessments.** While scoring individual CVEs is standard practice, advisories often bundle multiple vulnerabilities. Our study found that comprehensive advisory-level scores are uncommon, but when present, frequently represent only the maximum score of the included CVEs. This approach may not adequately capture the cumulative risk or the actual impact of applying a multi-vulnerability patch. Consequently, there is a need for more formal guidance or established methodologies for generating and evaluating meaningful advisory-level scores. Such practices could incorporate factors beyond the highest CVSS score, offering sysadmins a more holistic perspective for prioritizing remediation efforts.

**Encouraging adoption of, and investigating barriers to, machine-readable formats.** Our analysis revealed that an overwhelming majority of studied public advisories utilize unstructured formats (93.3%) like HTML web pages, hindering automated processing and efficient data aggregation. This reliance on manual extraction poses significant challenges for large-scale research and operational vulnerability management. Adopting standardized, machine-readable formats, such as CSAF or JSON, is essential for improving efficiency. Further investigation into the specific barriers preventing wider adoption—whether technical, financial, or organizational—would be beneficial to inform strategies to facilitate this transition across the ecosystem. While our study did not formally investigate these root causes, we hypothesize that these contribute to the adoption issues. Specifically, current legacy systems may result in structured data not being easily generated. Organizations, such as smaller ICSAs, that have a limited set of products may not have dedicated security teams or expertise to create advisories, instead relying on centralized organizations like CISA. Finally, organizational barriers such as simple inertia—an "if it isn't broken, don't fix it" mentality—can be a powerful impediment to change, especially when existing processes are deemed "good enough" for internal and legal purposes. Within resource-strapped security teams, the effort required to improve advisory formatting is often a lower priority than the core mission of analyzing and coordinating the remediation of the vulnerabilities themselves.

## Acknowledgements

We thank the anonymous reviewers who provided helpful comments on drafts of this paper. This project was supported by a gift from MedCrypt, NSF grant (2247959), and US Air Force contract (FA864924P0557).

## References

[1] Supplementary materials. https://osf.io/vfch3/?view_only=be45a1e2f8f74791b0ce565079ec1e24.

[2] Afsah Anwar, Ahmed Abusnaina, Songqing Chen, Frank Li, and David Mohaisen. Cleaning the NVD: Comprehensive quality assessment, improvements, and analyses. *IEEE Transactions on Dependable and Secure Computing*, 19(6):4255–4269, 2022.

[3] Ashish Arora, Ramayya Krishnan, Rahul Telang, and Yubao Yang. An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure. *Information Systems Research*, 21(1):115–132, 2010.

[4] Artur Balsam, Maciej Nowak, Michał Walkowski, Jacek Oko, and Sławomir Sujecki. Analysis of CVSS vulnerability base scores in the context of exploits' availability. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, pages 1–4. IEEE, 2023.

[5] Rob Barrett, Eser Kandogan, Paul P Maglio, Eben M Haber, Leila A Takayama, and Madhu Prabaker. Field studies of computer system administrators: Analysis of system management tools and practices. In *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, pages 388–395, 2004.

[6] Yogiraj Bhoomkar, Sushant Vernekar, Arya Kulkarni, Pranav Kulkarni, and Arun Aniyan. Knowledge graph of mergers and acquisitions. In *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pages 6–12, 2021.

[7] Bloomberg – Business News, Stock Markets, Finance, Breaking & World News. https://www.bloomberg.com/. Accessed: 2024-07-23.

[8] Brian Krebs. Funding Expires for Key Cyber Vulnerability Database – Krebs on Security.

[9] Center for Devices and Radiological Health, Food & Drug Administration. Postmarket Management of Cybersecurity in Medical Devices. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices, 2016.

[10] CERT@VDE. Advisories. https://cert.vde.com/en/advisories/. Accessed: 2024-05-14.

[11] CISA. US-CERT and ICS-CERT transition to CISA. https://www.cisa.gov/news-events/alerts/2023/02/24/us-cert-and-ics-cert-transition-cisa, February 2023. Accessed: 2024-07-11.

[12] Crunchbase. https://www.crunchbase.com/. Accessed: 2024-07-23.

[13] CVE Foundation. CVE Foundation launched to secure the future of the CVE program. https://www.thecvefoundation.org/.

[14] CVE numbering authorities. https://www.cve.org/ProgramOrganization/CNAs/, 2024. Accessed: 2024-06-27.

[15] Cybersecurity and Infrastructure Security Agency. BOD 19-02: Vulnerability remediation requirements for internet-accessible systems. https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-accessible-systems, April 2019.

[16] Cybersecurity and Infrastructure Security Agency. CISA CSAF repository. https://github.com/cisagov/CSAF, June 2024. Accessed: 2024-06-29.

[17] Cybersecurity and Infrastructure Security Agency (CISA). Coordinated Vulnerability Disclosure Program. https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program, 2025. Accessed: 2025-05-05.

[18] Stephanie de Smale, Rik van Dijk, Xander Bouwman, Jeroen van der Ham, and Michel van Eeten. No one drinks from the firehose: How organizations filter and prioritize vulnerability information. In *IEEE Symposium on Security and Privacy (Oakland)*, 2023.

[19] Ying Dong, Wenbo Guo, Yueqi Chen, Xinyu Xing, Yuqing Zhang, and Gang Wang. Towards the detection of inconsistencies in public security vulnerability reports. In *28th USENIX Security Symposium*, August 2019.

[20] Dave Dugal and Dale Rich. Common Vulnerability Scoring System Version 4.0. https://www.first.org/cvss/v4-0, June 2023.

[21] European Union Agency for Cybersecurity. European Union Vulnerability Database. https://euvd.enisa.europa.eu/homepage.

[22] Igor Forain, Robson de Oliveira Albuquerque, and Rafael Timóteo de Sousa Júnior. Towards system security: What a comparison of national vulnerability databases reveals. In *17th Iberian Conference on Information Systems and Technologies (CISTI)*, 2022.

[23] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner. Large-scale vulnerability analysis. In *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, 2006.

[24] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syad Asad Naqvi. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. In *IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, 2018.

[25] Christian Fruhwirth and Tomi Mannisto. Improving CVSS-based vulnerability prioritization and response with context information. In *3rd International Symposium on Empirical Software Engineering and Measurement (ESEM)*, 2009.

[26] Laurent Gallon. Vulnerability discrimination using CVSS framework. In *IFIP International Conference on New Technologies, Mobility and Security*, 2011.

[27] ICS-CERT. What is ICS-CERT? ICS-CERT Monthly Monitor, July/August 2011. Accessed: 2024-07-11.

[28] ICS-CERT. Medical devices hard-coded passwords. https://www.cisa.gov/news-events/ics-alerts/ics-alert-13-164-01, October 2013.

[29] Jay Jacobs, Sasha Romanosky, Octavian Suciu, Ben Edwards, and Armin Sarabi. Enhancing vulnerability prioritization: Data-driven exploit predictions with community-driven insights. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 194–206, 2023.

[30] Adam Jenkins, Linsen Liu, Maria Wolters, and Kami Vaniea. Not as easy as just update: Survey of system administrators and patching behaviours. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, 2024.

[31] Yuning Jiang, Manfred Jeusfeld, and Jianguo Ding. Evaluating the data inconsistency of open-source vulnerability repositories. In *Proceedings of the International Conference on Availability, Reliability and Security*, ARES, 2021.

[32] Pontus Johnson, Robert Lagerström, Mathias Ekstedt, and Ulrik Franke. Can the Common Vulnerability Scoring System be trusted? A Bayesian analysis. *IEEE Transactions on Dependable and Secure Computing*, 15(6):1002–1015, 2018.

[33] Philipp Kuehn, Markus Bayer, Marc Wendelborn, and Christian Reuter. OVANA: An approach to analyze and improve the information quality of vulnerability databases. In *Proceedings of the International Conference on Availability, Reliability and Security*, ARES, 2021.

[34] Yebin Lee and Youngjung Geum. Identifying patterns of mergers and acquisitions in startup: An empirical analysis using Crunchbase data. *IEEE Access*, 11:42463–42472, 2023.

[35] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini 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.

[36] Bharadwaj RK Mantha, Yeojin Jung, and B Garcia De Soto. Implementation of the common vulnerability scoring system to assess the cyber vulnerability in construction projects. In *Proc., Creative Construction E-Conf*, pages 117–124, 2020.

[37] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[38] Peter Mell, Karen Scarfone, and Sasha Romanosky. Common Vulnerability Scoring System. *IEEE Security & Privacy*, 4(6):85–89, 2006.

[39] Michael Schueler. Black and blue, or white and gold? - Minimizing vulnerability scoring discrepancies due to limited information. CVE/FIRST VulnCon 2024, March 2024.

[40] Lucas Miranda, Daniel Vieira, Leandro Pfleger de Aguiar, Daniel Sadoc Menasché, Miguel Angelo Bicudo, Mateus Schulz Nogueira, Matheus Martins, Leonardo Ventura, Lucas Senos, and Enrico Lovat. On the flow of software security advisories. *IEEE Transactions on Network and Service Management*, 18(2):1305–1320, 2021.

[41] MITRE. CVEProject/Cve-Schema.

[42] Priscilla Moriuchi and Bill Ladd. Pavlov's digital house: Russia focuses inward for vulnerability analysis. Technical report, Insikt Group - Recorded Future, July 2018.

[43] Vidya Murthy. Analysis: Assessing correlation between CVSS scores in vulnerability disclosures and patching. *Biomedical instrumentation & technology*, 54(1):44–46, 2020.

[44] National Vulnerability Database. CVE FAQs. https://nvd.nist.gov/general/FAQ-Sections/CVE-FAQs. Accessed: 2024-05-17.

[45] National Vulnerability Database. Vulnerability Metrics. https://nvd.nist.gov/vuln-metrics/cvss, March 2024. Accessed: 2024-05-17.

[46] Maciej Nowak, Michał Walkowski, and Sławomir Sujecki. Conversion of CVSS base score from 2.0 to 3.1. In *2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–3. IEEE, 2021.

[47] Maciej Nowak, Michał Walkowski, and Sławomir Sujecki. Machine learning algorithms for conversion of CVSS base score from 2.0 to 3.x.

In *International Conference on Computational Science*, pages 255–269. Springer, 2021.

[48] Nuclear Regulatory Commission. § 73.54 Protection of digital computer and communication systems and networks, March 2009. Accessed: 2024-07-11.

[49] OASIS. Common security advisory framework version 2.0. https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.md, November 2022.

[50] Office of the DoD Chief Information Officer. DOD INSTRUCTION 8531.01: DOD VULNERABILITY MANAGEMENT. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf, September 2020.

[51] Kevin Poireault. NVD Revamps Operations as Vulnerability Reporting Surges.

[52] Murugiah Souppaya and Karen Scarfone. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Technical Report NIST Special Publication (SP) 800-40 Rev. 4, National Institute of Standards and Technology, 2022.

[53] Jonathan Spring, Eric Hatleback, Allen Householder, Art Manion, and Deana Shick. Time to change the CVSS? *IEEE Security & Privacy*, 19(2):74–78, 2021.

[54] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. Didn't you hear me? – Towards more successful web vulnerability notifications. In *Network and Distributed System Security Symposium (NDSS)*, 2018.

[55] Tyler Terenzoni. Rapid7 offers continued vuln coverage in the face of NVD delays — Rapid7 Blog.

[56] Wikipedia. https://en.wikipedia.org/. Accessed: 2024-07-23.

[57] Julia Wunder, Andreas Kurtz, Christian Eichenmüller, Freya Gassmann, and Zinaida Benenson. Shedding light on cvss scoring inconsistencies: A user-centric study on evaluating widespread security vulnerabilities. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 1102–1121. IEEE, 2024.

[58] Siqi Zhang, Minjie Cai, Mengyuan Zhang, Lianying Zhao, and Xavier de Carné de Carnavalet. The flaw within: Identifying CVSS score discrepancies in the NVD. In *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 185–192. IEEE, 2023.