Severity vs Risk: The limitations of CVSS

MUHAMMAD RAFI ALBAB, University of Twente, The Netherlands

The CVSS is otherwise known as the Common Vulnerability Scoring System. Undoubtedly a standard in prioritizing and assessing software vulnerabilities. A structured approach and numerical scoring system vastly help evaluate vulnerabilities based on technical severity. Despite its popularity, the CVSS has limitations. For example, it often does not align with real-world exploitation trends or some specific needs of stakeholders like patch developers. This paper is a systematic literature review to identify and analyze these shortcomings, specifically the prioritization of vulnerabilities for risk management. Furthermore, the proposed solutions are analyzed to address these issues, including alternative frameworks with a comparative evaluation of their effectiveness. These findings aim to provide a better understanding of the limitations of CVSS and its potential for improvement in vulnerability prioritization practices.

Additional Key Words and Phrases: Risk Analysis, CVSS, Vulnerabilites

1 INTRODUCTION

New vulnerabilities are a common phenomenon that most technological companies and organizations experience. For many, the most straightforward approach to assess prioritization is to use Common *Vulnerability Scoring System* (CVSS), paying attention closely to the technical severity of each vulnerability. CVSS stands out among other vulnerability scoring systems and is widely regarded as the standard. CVSS provides a structured approach to evaluating vulnerabilities by assigning a quantitative score based on exploitability, impact, and environmental conditions. The newest version of CVSS is version *4.0* which includes new features such as improvement of finer granularity through the addition of new Base metrics and values. The newest update of the metric will be the version that's analyzed for this research[3].

1.1 CVE

CVE stands for Common Vulnerabilities and Exposures. The main goal of the CVE database is to give a standard identifier or name for the identified vulnerabilities. How CVSS is correlated to CVE is that CVSS is a score that depicts the severity of said CVE. It is a database that's hosted by MITRE[1] which provides a standardized list of publicly known information about security vulnerabilities and exposures. CVE is important to share data across various tools and repositories that are available in the security ecosystem[7] .

For a vulnerability to be published as a CVE a unique number is reserved for it, then when the time comes to publish the CVE that unique number will be assigned it. The format of the unique CVE number is CVEyear-4 digit number. The CVE part of the unique number is a fixed prefix that all published CVE vulnerabilities will have [1].

1.2 How CVSS works

CVSS provides a numerical score ranging from 0 - 10 that reflects the severity and vulnerability that enables organizations to prioritize based on the response. The severity scale for CVSS can be seen in 1

Table 1. Severity Scale for CVSS

Severity	Base Score
None	0
Low	<4.0
Medium	<7.0
High	<9.0
Critical	<= 10.0

There are a few metrics that determine the score of CVSS, it consists of four metric groups namely Base, Threat, Environmental, and the newest metric that's introduced in the newest version 4.0 which is Supplemental [1].

1.2.1 Base Metrics. The base metrics reflect the intrinsic characteristics of a vulnerability that doesn't change over time or across the environment. The base metric itself consists of exploitability metrics and impact metrics. Exploitability measures how easily the vulnerability is compromised in a technical sense, while the impact metric evaluates the aftermath of a successful exploit [1].

1.2.2 Threat Metrics. The threat metric represents the features of the vulnerability that can vary over time but it's not altered by different user environments meaning that it only evaluates aspects of the current state. For example, it doesn't take into account a release of an official patch. A release of an official patch will make the threat metrics score lower while an easy-to-use exploitation kit will increase the score [1].

1.2.3 Environmental Metrics. The environmental metrics help to modify the score based on the organization's security environment. The environmental metrics consist of two sub-categories which are security requirements and modified base metrics [1].

Security Requirements. Security requirements follow the business needs by modifying confidentiality, integrity, and availability. Modified base metrics

Modified Base Metrics. The individual base metrics are changed based on the user's environmental abilities such his the user's ability to mitigate attacks.

1.2.4 Supplemental Metrics. Supplemental metrics add more context to the vulnerability score. It provides additional extrinsic characteristics while not changing the final score. The context that can be provided for the supplemental metrics includes the following:

[1] https://cve.mitre.org/

TScIT 37, July 8, 2022, Enschede, The Netherlands

Safety metrics, automated metrics, Provider Urgency, Recovery, Value Density, and Vulnerability Response Effort [1].

1.3 Why CVSS is not suitable for risk management

Spring [12] suggests that the CVSS algorithm is not justified, either formally or empirically. According to the specifications of CVSS, using the score directly as a risk score is a mistake. However, some compliance bodies recommend using the score as a risk assessment analysis score. An example is the U.S. government. The suggestion of using the CVSS score as a risk management score, not as it was intended, can be seen via the National Institute of Standards and Technology (NIST) guidance. An example of such guidance can be seen in Special Publications 800-115, pages 7-4 and 800-40r3, page 4) [11].

2 PROBLEM STATEMENT

As mentioned above in Why CVSS is not suitable for risk management, CVSS is being misused as a score for risk management. While CVSS is meant to be used to assess severity instead of risk, even organizational bodies suggest that CVSS is adequate for risk management.

The Common Vulnerability Scoring System is widely recognized as the industry standard for evaluating software vulnerabilities. The scoring system provides a structured approach by assigning numerals to vulnerabilities, enabling organizations to prioritize security threats based on severity. While CVSS is widely used for vulnerability assessment, it has significant limitations in risk management, as it primarily measures severity rather than actual exploitation risk. Given that statement, the following research questions are made:

(1) What are the limitations of CVSS in prioritizing vulnerabilities for risk management?
(2) What are the possible solutions to the limitations of CVSS in prioritizing vulnerabilities for risk management?

3 METHODOLOGY

A big part of this research would be a literature review. The methodology used to conduct this research paper is a literature review to find issues about the topic and to give insights into how previous projects have been done to tackle a similar issue [10].

3.1 Data collection

3.1.1 Systematic Literature Review. To collect data on this topic, using online databases such as ACM Digital Library, Scopus, and Google Scholar. This would suit best for this research as it allows for a filtration system that ensures the use of peer-reviewed sources. The three databases have been chosen as they are the most popular repository with substantial information and content. To find the most relevant resources, the following search queries and search criteria were chosen:

Inclusion and Exclusion Criteria:

- Not peer-reviewed papers in their respective repository are excluded
- Papers not written in English are excluded
- Papers focusing on a certain case study are included

Keywords that would be used:

"CVSS limitations" AND ("vulnerability prioritization" OR "risk management") AND ("alternative methods" OR "solutions") AND "case study"

Search result:

- Scopus: 5
- ACM Digital Library: 0
- Google Scholar: 0

From the limited number of results that can be seen in Systematic Literature Review the queries give very limited hits even without filtering out the search with search criteria such as publication year, which would be relevant for the study as it would determine the version of CVSS. Without the external search criteria, the search only resulted in 5 papers in total all coming from the same database which is Scopus. All the search results that Scopus was able to generate was all relevant to the research content-wise and in an acceptable year of publication. Therefore, no further filtration and selection needs to be done.

3.2 Limitations of CVSS

As discussed in the introduction section briefly, although CVSS is a great standard for its use case, it has plenty of limitations to improve on in prioritizing vulnerabilities. The introduction section gives a brief overview and example of the limitations of CVSS. To have a broader view of the limitations of CVSS, relevant work must be analyzed through a literature review.

When looking at the limitations of CVSS, it is important to take into account the different versions that were used. The literature might review an outdated version of CVSS that might have already been implemented. To understand what the newest CVSS version offers as it is on the verge of updating to the new version of CVSS which is version 4.0 [3], literature about the limitations and solutions of CVSS needs to take into account the version it might be outdated and those limitations might already be implemented in the newest version.

3.3 Solutions to Limitations

To find the means to solve the issues of CVSS, relevant literature of the sort would be the basis of solving the limitations of CVSS in risk management. Literature of solutions such as [13] would be the basis for improving vulnerability prioritization. More literature will be analyzed to come up with the best solution for each of the problems that are discovered in the first research question which is the limitations of CVSS for prioritizing vulnerabilities. Understanding the solutions of past research papers by researchers on this topic and understanding why it's important and assessing if the solution is indeed feasible will also be done during this part of the research.

4 LITERATURE REVIEW

4.1 Limitations of CVSS

Before conducting the literature review for the limitations of CVSS in risk management, the version of CVSS needs to be predetermined as the version of CVSS matters to analyze the limitations of CVSS in risk management. This section is also mentioned briefly in the methodology section of the paper. The latest version of CVSS is 4.0.

The latest version of CVSS 4.0 has new features that also consider risk management. The new introduction of CVSS considers a combination of the base score with a score of threat and environmental score How CVSS works. However, all of the related work analyzed in this section is during the period where the latest version is CVSS 3.0 besides [2] (version 2.0), since during the time of this research CVSS 4.0 was very new. That being said, all of the works mentioned here are still relevant at the time of this research.

4.1.1 Effectiveness of CVSS in the wild. According to Allodi and Massacci [2] when studying the effectiveness of CVSS in the wild, they found that CVSS score doesn't correspond to real-world exploitation, and exploitation with medium and low CVSS scores are still frequently exploited [5]. Borgozi et al. [4] showed (as a side result) that CVSS sub-score distribution doesn't correlate well with the existence of known exploits. This result can be interpreted in two ways: the exploitability of CVSS uses the wrong metric, or Borzogi and his coauthors use the wrong database. For example, ExploitDB was used by other security researchers to show their skills for penetration testing, but it might not have had any correlation with actual hackers. The paper shows CVSS as a standard for assessing vulnerability risk, and it shows poor predictive power for exploitations in the wild. In conclusion, the paper concludes that the CVSS scores are inadequate to prioritize vulnerabilities based on the risk of exploitation in the real world.

4.1.2 Quantitative output that lacks context. ¢CVSS centers on technical severity as the primary metric1, but it does not adequately guide stakeholders on how to use these scores to make informed decisions about vulnerability management. This disconnect leaves organizations without a clear pathway from severity scores to actionable steps, reducing the system's practical utility [13]. The use of numerical scores in CVSS creates a misleading sense of precision. Scores often overlap due to inherent errors and ambiguities, making it difficult to distinguish between categories like "high" and "critical." This lack of clarity undermines confidence in the system's prioritization and can lead to inconsistent decision-making [13]. CVSS adopts a generalized approach that fails to consider the diverse contexts in which vulnerabilities exist. Temporal, environmental, and stakeholder-specific factors are either optional or insufficiently integrated, limiting the system's ability to provide relevant guidance tailored to the unique needs of different industries or organizational roles[13]. The process behind CVSS scoring lacks transparency, making it difficult for non-experts to understand, troubleshoot, or justify decisions based on the scores. Additionally, its one-size-fits-all framework does not accommodate the varied priorities of stakeholders, forcing all users into a rigid and often impractical system [13].

4.1.3 Impractical and inefficient for large-scale vulnerability management. The assessment of possible exploitations and the impact of vulnerability over time is calculated using the temporal scoring of CVSS. However, CVSS does not automatically update these values, leading to inefficiencies in tracking evolving threats. Jung et al. [6] mentioned that even the use of automatic calculation for the temporal scoring of CVSS is not sufficient to measure security risks. Implementing automatic calculation for temporal risk management does not prioritize vulnerabilities and requires manual labor from the SOC. Due to the extensive amount of manual labor, Zhang [15] mentioned that unstructured priorities and complications would arise such as human errors or oversights. The notorious case of Equifax data breach is an example of human error. Due to an oversight in patching before exploitation by a malicious actor [8].

4.1.4 Limitation: Static Nature of CVSS Scoring System. The static nature of the Common Vulnerability Scoring System (CVSS) significantly hinders effective cybersecurity risk management due to its two main limitations: fixed scoring and non-responsiveness to new information. Initially, when a vulnerability is identified, CVSS assigns a score based on the information available at that time, encapsulating factors like exploitability and impact [14]. This score remains unchanged, which is problematic because it does not reflect subsequent developments that could affect the threat's severity. For example, if a new exploit tool is developed that makes a previously complex vulnerability easy to exploit, the static nature of CVSS means that the score does not adjust to reflect this increased risk. This could lead organizations to underestimate the urgency of addressing the vulnerability, leaving systems exposed to potential attacks. Therefore, organizations must integrate continuous threat intelligence and real-time monitoring to ensure that their vulnerability assessments remain current and accurately reflect the evolving landscape of cybersecurity threats.

4.2 Solutions to Limitations

4.2.1 Data Driven Approach. Jonathan et al. [13] propose a data-driven approach by using the Stakeholder-Specific Vulnerability Categorization (SSVC) as a solution to the problem that was mentioned in Quantitative output that lacks context section. The author proposed a replacement for the numerical score with a qualitative decision tree that is tailored for specific stakeholder groups such as patch developers and patch appliers. The output is qualitative such as "Defer", "Out-of-Band", or "Immediate". The unique stakeholder groups had unique decision trees that reflect their priorities and responsibilities which would ensure the appropriate context guidance for vulnerability management. The decision-making framework is transparent, with clear documentation for each decision point and its rationale. The methodology that's displayed for the decision trees aims to be explainable to competent non-experts to facilitate a better understanding and adoption. The framework is designed as a foundation that encourages empirical testing, refinement, and adaptation by the community. The solution emphasizes managing the diversity of stakeholder needs while being practical and accessible.

4.2.2 Context Aware Vulnerability Prioritization Model. Jung et al. [6] suggest that the limitations of CVSS lie in the lack of effectiveness of the temporal scoring as mentioned in the previous section of this paper Limitations of CVSS. Jung et al. propose a context-aware vulnerability prioritization (CAVP) model. The model aims to tackle two design considerations. The first design consideration is to improve the existing CVSS metric by implementing the temporal characteristics of the vulnerabilities. The second design consideration is to provide a step-by-step process of vulnerability prioritization that allows CAVP to be integrated within the organization's risk management workflow. The following are the steps of the CAVP model:

CVE Database Construction and Analysis. The first step in the proposed Context-Aware Vulnerability Prioritization (CAVP) model involves constructing a centralized database of known vulnerabilities by leveraging data from the National Vulnerability Database (NVD). This database includes critical details about each Common Vulnerability and Exposure (CVE) 11, such as descriptions, severity scores, associated references (URLs), and resource tags (e.g., vendor advisories, patches, or technical descriptions). The model incorporates a systematic analysis of the credibility and relevance of these references. For instance, URLs originating from authoritative sources, such as software vendors or trusted vulnerability databases, are prioritized. The goal of this step is to provide a robust foundation for evaluating vulnerabilities by incorporating both static and evolving contextual information.

Environmental Vulnerability Scan. The second step focuses on tailoring the analysis to the organization's unique IT environment. By matching the CVEs in the constructed database to the specific IT assets within an organization, the model filters out irrelevant vulnerabilities and focuses on those that pose a tangible risk. During this process, the organization's Security Operations Center (SOC) team assigns security requirement ratings to assets based on their importance for confidentiality, integrity, and availability. Additionally, existing mitigation measures, such as firewalls or access controls, are considered to adjust the vulnerability's impact on the environment. This step not only reduces the noise of irrelevant vulnerabilities but also prioritizes those that are critical to the organization's operational security.

Context-Aware Vulnerability System. The heart of the CAVP model is the enhanced scoring system, CAVSS, which improves upon the traditional CVSS by automating the calculation of temporal metrics. These temporal metrics—Exploit Code Maturity (ECM), Remediation Level (RL), and Report Confidence (RC)—are derived using a set of expert-validated heuristic rules. The CAVSS integrates these temporal metrics with the CVSS Base Score and environmental factors to produce a comprehensive, context-aware vulnerability score. This score reflects not only the technical severity of a vulnerability but also its relevance and urgency in the organization's specific context.

Vulnerability Prioritization Visualization. The final step involves presenting the prioritized vulnerabilities through an intuitive visualization tool designed to aid decision-making. This tool organizes vulnerabilities into summary charts, highlighting overall scores, temporal scores, and environmental scores. It allows users to interactively filter and drill down into specific vulnerabilities for detailed information. For example, decision-makers can access hyperlinks to trusted sources for remediation details or investigate why certain vulnerabilities have escalated in severity. The visualization also provides clear indicators for severity changes, helping the SOC team focus on the most critical vulnerabilities. By integrating this visualization into the workflow, organizations can streamline their mitigation efforts, ensuring that limited resources are directed to the most pressing risks.

4.3 Related Works

Setiawan et al [9] explores the gap between CVSS and risk assessment to create a risk assessment framework for web-based applications of local government. Their strategy involved evaluating various methods to address the problem and identify the optimal solutions based on their analysis. Although CVSS is effective in measuring the severity of vulnerabilities, it does not account for key risk factors such as the likelihood of exploitation and contextual asset sensitivity, which are critical for a comprehensive risk assessment. The author presents CVSS's lack of contextual awareness and reliance on subjective judgments for likelihood estimation. Because of that limitation, CVSS is insufficient for accurately prioritizing risks in complex environments.

Overcoming these challenges, Setiawan et al. [9] integrate CVSS with additional methods such as the CAPEC dictionary for likelihood assessment and the asset sensitivity form to evaluate the contextual importance of the affected systems. The author's proposed framework introduces a hybrid risk model that combines CVSS for the common vulnerabilities, CAPEC for the likelihood, and sensitivity using asset profiling into one single quantitative matrix. The framework that the author provides was successfully tested on a local environment application which yields improved risk prioritization actionable insights. The approach that the author proposed, demonstrates how augmenting CVSS with tools that complement it and context-specific factors can address its inherent limitations and provide a more effective basis for risk management.

5 RESULT

5.1 Findings

From the findings made by means of a literature review in the section Limitations of CVSS and Solutions to Limitations a table is made as a result to give a clear overview of the limitations and solution, this can be seen 2. Surprisingly, all of the papers that were found gave a different approach to tackling different limitations. One common factor that can be deduced from the different research that is made by those papers is that CVSS are further implemented based on the limitations that they found are relevant to their respective cases.

Table 2 highlights different limitations and the solution according to their given author. In summary, the limitations are the inefficiency of CVSS in large-scale vulnerability management, the static nature of CVSS scoring, the lack of real-time adaptability, and the inability to factor in evolving threat intelligence making the tool impractical, especially for dynamic risk management. While it can be seen that there are clear flaws in the use of CVSS in risk management the effort to solve these issues is lacking. It can be seen in Systematic Literature Review that the amount of research on this matter is concerning. The research fortunately provided alternative models to help tackle their respective issues.

5.2 Lack of Sources

CVSS is widely accepted as the standard for assessing vulnerabilities. Although it's not perfect and there are a lot of papers backing this which were mentioned in Why CVSS is not suitable for risk management, specifically for risk management it's not explored thoroughly. As it is the industry standard that's used for assessing

Title	Author	Year	Limitation	Solution
A preliminary analysis of vulnerability scores for attacks in wild: the ekits and sym dataset	Luca Allodi and Fabio Massacci's	2012	Poor predictive power for exploitation in the wild	-
CAVP: A context-aware vulnerability prioritization model	Jung, Bill, et al.	2022	Impractical and inefficient for large-scale vulnerability management due to lack of automation in temporal scoring.	A context-aware vulnerability prioritization (CAVP) model
Designing a Cybersecurity Risk Assessment Framework for Local Government Web-Based Applications	Setiawan et al.	2023	The gap between CVSS and risk assessment, does not account for key risk factors such as the likelihood of exploitation and contextual asset sensitivity.	Framework for risk assessment
Prioritizing Vulnerability Response: A Stakeholder Specific Vulnerability Categorization	Jonathan et al.	2019	It emphasizes technical severity without providing clear guidance on translating scores into actionable decisions for stakeholders.	Data-driven approach by using Stakeholder-Specific Vulnerability Categorization (SSVC)

Table 2. Comparison of vulnerability analysis and prioritization models.

vulnerabilities and has few alternatives that rivals it reduces the need to focus on finding its flaws or alternatives.

There might be a gap between the practical, industry-driven use of CVSS and the theoretical, research-based analysis of its limitations and solutions. Industry users might encounter and address issues with CVSS in practical, undocumented ways that do not contribute to academic literature.

6 DISCUSSION

6.1 Limitation of this research

6.1.1 Time Constraints. One of the main obstacles when conducting this thesis was a limitation in time, which impacted the study on the data collection effect, analysis, and validation of findings. Performing a thorough and intensive it requires extensive data from real-world cybersecurity incidents. Performing such a task is time-intensive to gather and analyze. Given the amount of time allocated, this research relies on available research of selected case studies rather than a long-term empirical observation across diverse organizations.

Time limitations also affect the depth of testing for alternative models. While frameworks like SSVC and CAVP are explored as potential solutions, a longitudinal study to keep track of their effectiveness over time in a real-world security environment would provide a more conclusive validation. Due to a shorter timeline, this thesis focuses on findings already present in the literature rather than continuous monitoring of security outcomes. Performing a large-scale test environment across different industries to validate results comprehensively is beyond the scope of this research.

6.2 Version of CVSS

The current study of this topic is based on the current and slightly outdated version of CVSS, which are version 3.0 to 4.0. Future revisions of the scoring system may fix the current shortcomings of CVSS. However, one thing to be noted is that this research started during the adaptation to 4.0 as it was just released shortly before this research was done. That being said, a new version will not be released for at least a few years. Going back to the release date of the newest version, since it is very recent there is a chance that a new solution to one of the shortcomings of CVSS is released once the newest version is explored more.

6.3 Future Work

6.3.1 Risk Test. As mentioned in the literature review and introduction Why CVSS is not suitable for risk management and often misused for risk management despite its being designed to measure severity rather than actual risk. Several regulatory bodies such as NIST have implicitly suggested using CVSS as a proxy for risk prioritization. However, research has shown this approach has indicated that this approach can lead to improper prioritization of vulnerabilities. In the future, knowing how relevant it is to be aware of CVSS misuse for risk management, a test on how fatal it is to use CVSS in a non-proper manner with actual data to support it by doing a systematic evaluation is needed to quantify real-world consequences of CVSS misuse. By conducting an empirical study, we can provide concrete evidence demonstrating the risks associated with misapplying CVSS as a risk management tool.

6.3.2 Horizontal Comparison of the solution. One of the key areas for future research is a comparative assessment of the alternative prioritization model beyond CVSS. This study highlights some limitations of CVSS when in a real-world situation a more detailed evaluation of each model mentioned in the Solutions to Limitations section is needed.

Future comparative assessment work should explore how these alternative models can be integrated into existing security operations, particularly in organizations that currently use CVSS as a way to measure risk assessment and other risk assessment tasks. Analyzing the feasibility of combining multiple methods such as SSVC for decision-making transparency and CAVP for automation, and additionally, a side-by-side comparison of these models in controlled simulations could provide insights into the practicality, scalability, and industry adoption potential.

7 CONCLUSION

The research conducted highlights the limitations of CVSS as a risk management tool. The research emphasizes the main function of CVSS being a severity assessment system rather than a comprehensive risk prioritization framework. While CVSS provides a standardized approach for scoring vulnerabilities it lacks features that make it a feasible risk management tool due to its static nature, lack of real-world exploitability considerations, and misalignment with risk-based decision-making.

Through a literature review, this research explores alternative approaches to risk assessment using CVSS as a foundation. These approaches consist of SSVC, CAVP, and hybrid risk framework models which are summarized in 2 that address many of the CVSS shortcomings. However, challenges remain in terms of the complexity of implementation, creating a new industry standard, and an extensive test of data outputs.

That being said, this research serves its purpose, shedding light on CVSS shortcomings in risk management and providing different alternative approaches. By integrating context-aware, dynamic, and stakeholder-specific models, cybersecurity professionals can make more informed decisions, allocate resources effectively, and enhance their overall security posture against evolving threats.

8 AI STATEMENT

During the preparation of this work, the author used ChatGPT in assisting the creation Latex table, Latex elements, and clarifying things about the topics that author finds difficult to understand. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.

REFERENCES

[1] Manuj Aggarwal. 2023. A Study of CVSS v4.0: A CVE Scoring System. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 14–16. https://doi.org/10.1109/IC3I59117.2023.10397701

[2] Luca Allodi and Fabio Massacci. 2012. A preliminary analysis of vulnerability scores for attacks in wild: the ekits and sym datasets. In *ACM Conferences*. Association for Computing Machinery, New York, NY, USA, 17–24. https://doi.org/10.1145/2382416.2382427

[3] Dale Rich Dave Dugal. 2024. Common Vulnerability Scoring System. https://www.first.org/cvss/v4-0 [Online; accessed 22. Nov. 2024].

[4] Bozorgi et al. 2024. OffSecs Exploit Database Archive. https://www.exploit-db.com [Online; accessed 19. Nov. 2024].

[5] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner. 2006. Large-scale vulnerability analysis. In *ACM Other conferences*. Association for Computing Machinery, New York, NY, USA, 131–138. https://doi.org/10.1145/1162666.1162671

[6] Bill Jung, Yan Li, and Tamir Bechor. 2022. CAVP: A context-aware vulnerability prioritization model. *Computers & Security* 116 (May 2022), 102639. https://doi.org/10.1016/j.cose.2022.102639

[7] Stephan Neuhaus and Thomas Zimmermann. 2010. Security Trend Analysis with CVE Topic Models. In *2010 IEEE 21st International Symposium on Software Reliability Engineering*. IEEE, 01–04. https://doi.org/10.1109/ISSRE.2010.53

[8] United States Government Accountability Office. 2018. "Data protection: actions taken by equifax and federal agencies in response to the 2017 Breach. https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf [Online; accessed 11. Dec. 2024].

[9] Edoh Setiawan, Lukito Edi Nugroho, and Rudy Hartanto. 2023. Designing a Cybersecurity Risk Assessment Framework for Local Government Web-Based Applications. In *2023 2nd International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*. IEEE. https://doi.org/10.1109/COSITE60233.2023.10249788

[10] Hannah Snyder. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research* 104 (Nov. 2019), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

[11] Murugiah Souppaya and Karen Scarfone. 2022. *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.* Special Publication 800-40 Revision 3. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-40r3

[12] Jonathan Spring, Eric Hatleback, Allen Householder, Art Manion, and Deana Shick. 2021. Time to Change the CVSS? *IEEE Secur. Priv.* 19, 2 (March 2021), 74–78. https://doi.org/10.1109/MSEC.2020.3044475

[13] Jonathan M. et al. Spring. 2019. Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization. https://insights.sei.cmu.edu/library/prioritizing-vulnerability-response-a-stakeholder-specific-vulnerability-categorization [Online; accessed 20. Nov. 2024].

[14] Panagiotis Vlachos. 2023. *BRIDGING THE GAP IN VULNERABILITY MANAGEMENT : A tool for centralized cyber threat intelligence gathering and analysis.* Luleå University of Technology. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1764197&dswid=-482

[15] Fengli Zhang, Philip Huff, Kylie McClanahan, and Qinghua Li. 2020. A Machine Learning-based Approach for Automated Vulnerability Remediation Analysis. In *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2020–01. https://doi.org/10.1109/CNS48642.2020.9162309