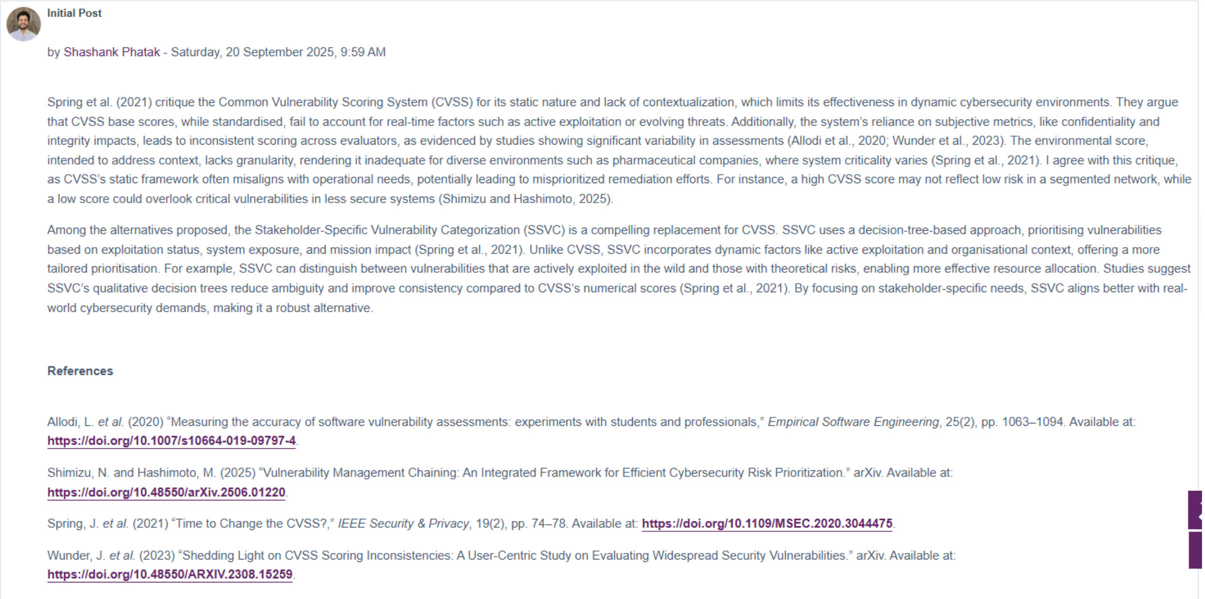
Collaborative Discussion 2

Initial Post



Initial Post

by Shashank Phatak - Saturday, 20 September 2025, 9:59 AM

Spring et al. (2021) critique the Common Vulnerability Scoring System (CVSS) for its static nature and lack of contextualization, which limits its effectiveness in dynamic cybersecurity environments. They argue that CVSS base scores, while standardised, fail to account for real-time factors such as active exploitation or evolving threats. Additionally, the system's reliance on subjective metrics, like confidentiality and integrity impacts, leads to inconsistent scoring across evaluators, as evidenced by studies showing significant variability in assessments (Allodi et al., 2020; Wunder et al., 2023). The environmental score, intended to address context, lacks granularity, rendering it inadequate for diverse environments such as pharmaceutical companies, where system criticality varies (Spring et al., 2021). I agree with this critique, as CVSS's static framework often misaligns with operational needs, potentially leading to misprioritized remediation efforts. For instance, a high CVSS score may not reflect low risk in a segmented network, while a low score could overlook critical vulnerabilities in less secure systems (Shimizu and Hashimoto, 2025).

Among the alternatives proposed, the Stakeholder-Specific Vulnerability Categorization (SSVC) is a compelling replacement for CVSS. SSVC uses a decision-tree-based approach, prioritising vulnerabilities based on exploitation status, system exposure, and mission impact (Spring et al., 2021). Unlike CVSS, SSVC incorporates dynamic factors like active exploitation and organisational context, offering a more tailored prioritisation. For example, SSVC can distinguish between vulnerabilities that are actively exploited in the wild and those with theoretical risks, enabling more effective resource allocation. Studies suggest SSVC's qualitative decision trees reduce ambiguity and improve consistency compared to CVSS's numerical scores (Spring et al., 2021). By focusing on stakeholder-specific needs, SSVC aligns better with real-world cybersecurity demands, making it a robust alternative.

References

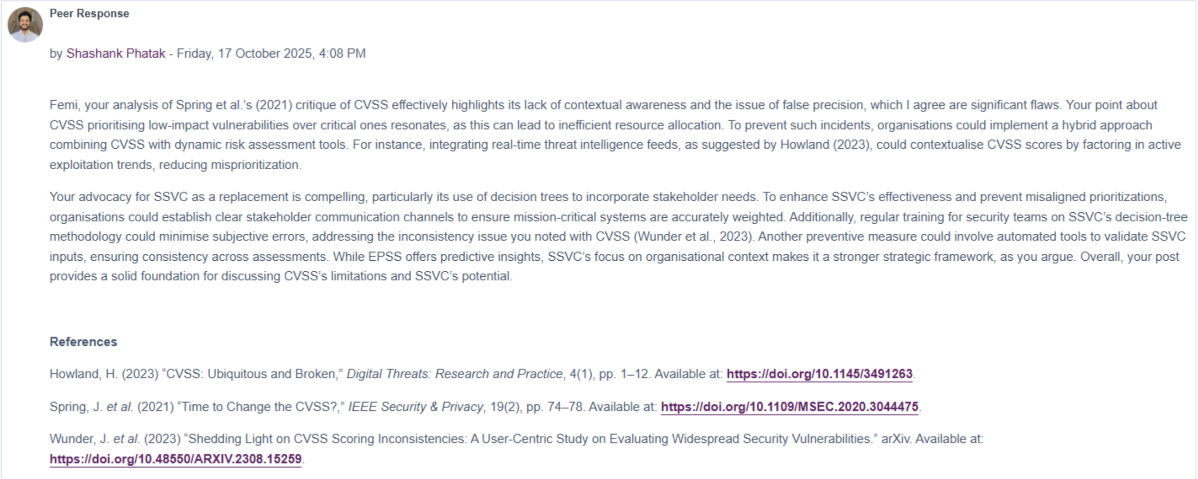
Allodi, L. *et al.* (2020) "Measuring the accuracy of software vulnerability assessments: experiments with students and professionals," *Empirical Software Engineering*, 25(2), pp. 1063–1094. Available at: **https://doi.org/10.1007/s10664-019-09797-4**.

Shimizu, N. and Hashimoto, M. (2025) "Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization." arXiv. Available at: **https://doi.org/10.48550/arXiv.2506.01220**.

Spring, J. *et al.* (2021) "Time to Change the CVSS?," *IEEE Security & Privacy*, 19(2), pp. 74–78. Available at: **https://doi.org/10.1109/MSEC.2020.3044475**.

Wunder, J. *et al.* (2023) "Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities." arXiv. Available at: **https://doi.org/10.48550/ARXIV.2308.15259**.

Peer Response to Femi Olowe



Peer Response

by Shashank Phatak - Friday, 17 October 2025, 4:08 PM

Femi, your analysis of Spring et al.'s (2021) critique of CVSS effectively highlights its lack of contextual awareness and the issue of false precision, which I agree are significant flaws. Your point about CVSS prioritising low-impact vulnerabilities over critical ones resonates, as this can lead to inefficient resource allocation. To prevent such incidents, organisations could implement a hybrid approach combining CVSS with dynamic risk assessment tools. For instance, integrating real-time threat intelligence feeds, as suggested by Howland (2023), could contextualise CVSS scores by factoring in active exploitation trends, reducing misprioritization.

Your advocacy for SSVC as a replacement is compelling, particularly its use of decision trees to incorporate stakeholder needs. To enhance SSVC's effectiveness and prevent misaligned prioritizations, organisations could establish clear stakeholder communication channels to ensure mission-critical systems are accurately weighted. Additionally, regular training for security teams on SSVC's decision-tree methodology could minimise subjective errors, addressing the inconsistency issue you noted with CVSS (Wunder et al., 2023). Another preventive measure could involve automated tools to validate SSVC inputs, ensuring consistency across assessments. While EPSS offers predictive insights, SSVC's focus on organisational context makes it a stronger strategic framework, as you argue. Overall, your post provides a solid foundation for discussing CVSS's limitations and SSVC's potential.

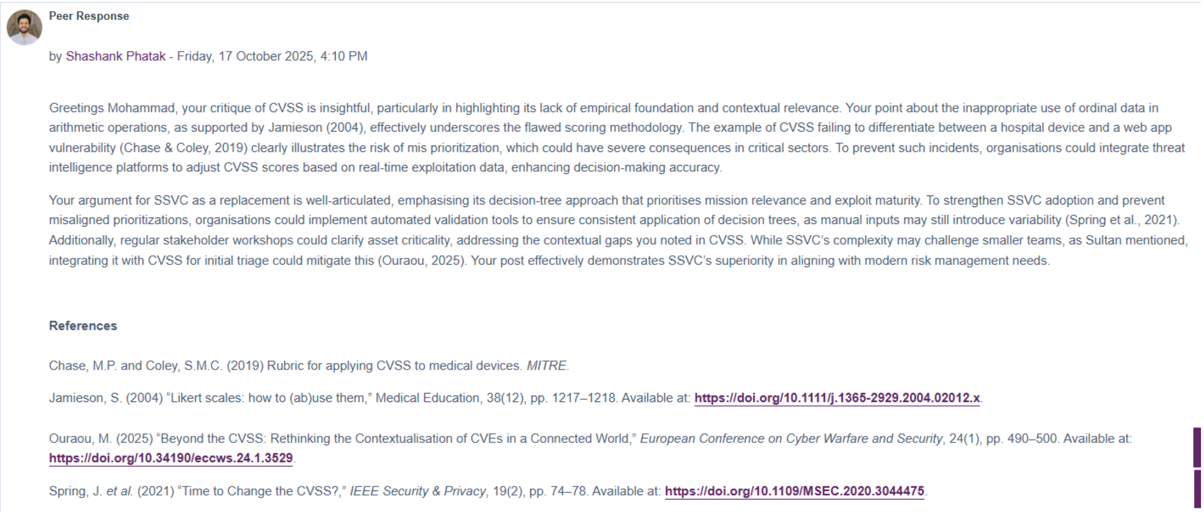
References

Howland, H. (2023) "CVSS: Ubiquitous and Broken," *Digital Threats: Research and Practice*, 4(1), pp. 1–12. Available at: **https://doi.org/10.1145/3491263**.

Spring, J. *et al.* (2021) "Time to Change the CVSS?," *IEEE Security & Privacy*, 19(2), pp. 74–78. Available at: **https://doi.org/10.1109/MSEC.2020.3044475**.

Wunder, J. *et al.* (2023) "Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities." arXiv. Available at: **https://doi.org/10.48550/ARXIV.2308.15259**.

Peer Response to Mohammad Ali Okleh Harahsheh



Peer Response

by Shashank Phatak - Friday, 17 October 2025, 4:10 PM

Greetings Mohammad, your critique of CVSS is insightful, particularly in highlighting its lack of empirical foundation and contextual relevance. Your point about the inappropriate use of ordinal data in arithmetic operations, as supported by Jamieson (2004), effectively underscores the flawed scoring methodology. The example of CVSS failing to differentiate between a hospital device and a web app vulnerability (Chase & Coley, 2019) clearly illustrates the risk of mis prioritization, which could have severe consequences in critical sectors. To prevent such incidents, organisations could integrate threat intelligence platforms to adjust CVSS scores based on real-time exploitation data, enhancing decision-making accuracy.

Your argument for SSVC as a replacement is well-articulated, emphasising its decision-tree approach that prioritises mission relevance and exploit maturity. To strengthen SSVC adoption and prevent misaligned prioritizations, organisations could implement automated validation tools to ensure consistent application of decision trees, as manual inputs may still introduce variability (Spring et al., 2021). Additionally, regular stakeholder workshops could clarify asset criticality, addressing the contextual gaps you noted in CVSS. While SSVC's complexity may challenge smaller teams, as Sultan mentioned, integrating it with CVSS for initial triage could mitigate this (Ouraou, 2025). Your post effectively demonstrates SSVC's superiority in aligning with modern risk management needs.

References

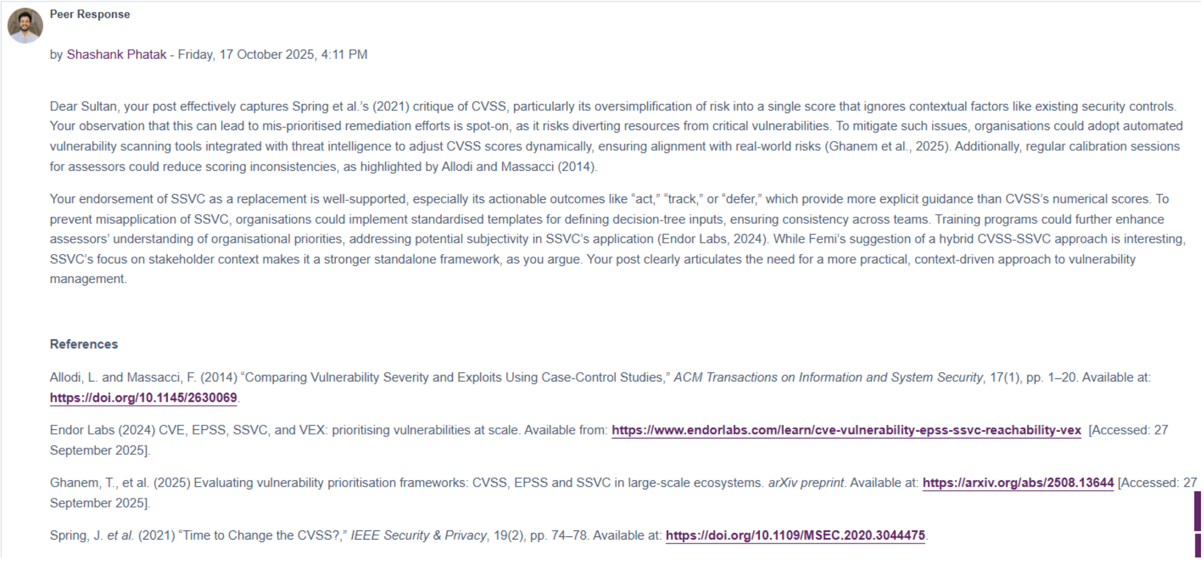
Chase, M.P. and Coley, S.M.C. (2019) Rubric for applying CVSS to medical devices. *MITRE*.

Jamieson, S. (2004) "Likert scales: how to (ab)use them," Medical Education, 38(12), pp. 1217–1218. Available at: **https://doi.org/10.1111/j.1365-2929.2004.02012.x**.

Ouraou, M. (2025) "Beyond the CVSS: Rethinking the Contextualisation of CVEs in a Connected World," *European Conference on Cyber Warfare and Security*, 24(1), pp. 490–500. Available at: **https://doi.org/10.34190/eccws.24.1.3529**.

Spring, J. *et al.* (2021) "Time to Change the CVSS?," *IEEE Security & Privacy*, 19(2), pp. 74–78. Available at: **https://doi.org/10.1109/MSEC.2020.3044475**.

Peer Response to Sultan Alaryani



Peer Response

by Shashank Phatak - Friday, 17 October 2025, 4:11 PM

Dear Sultan, your post effectively captures Spring et al.'s (2021) critique of CVSS, particularly its oversimplification of risk into a single score that ignores contextual factors like existing security controls. Your observation that this can lead to mis-prioritised remediation efforts is spot-on, as it risks diverting resources from critical vulnerabilities. To mitigate such issues, organisations could adopt automated vulnerability scanning tools integrated with threat intelligence to adjust CVSS scores dynamically, ensuring alignment with real-world risks (Ghanem et al., 2025). Additionally, regular calibration sessions for assessors could reduce scoring inconsistencies, as highlighted by Allodi and Massacci (2014).

Your endorsement of SSVC as a replacement is well-supported, especially its actionable outcomes like "act," "track," or "defer," which provide more explicit guidance than CVSS's numerical scores. To prevent misapplication of SSVC, organisations could implement standardised templates for defining decision-tree inputs, ensuring consistency across teams. Training programs could further enhance assessors' understanding of organisational priorities, addressing potential subjectivity in SSVC's application (Endor Labs, 2024). While Femi's suggestion of a hybrid CVSS-SSVC approach is interesting, SSVC's focus on stakeholder context makes it a stronger standalone framework, as you argue. Your post clearly articulates the need for a more practical, context-driven approach to vulnerability management.

References

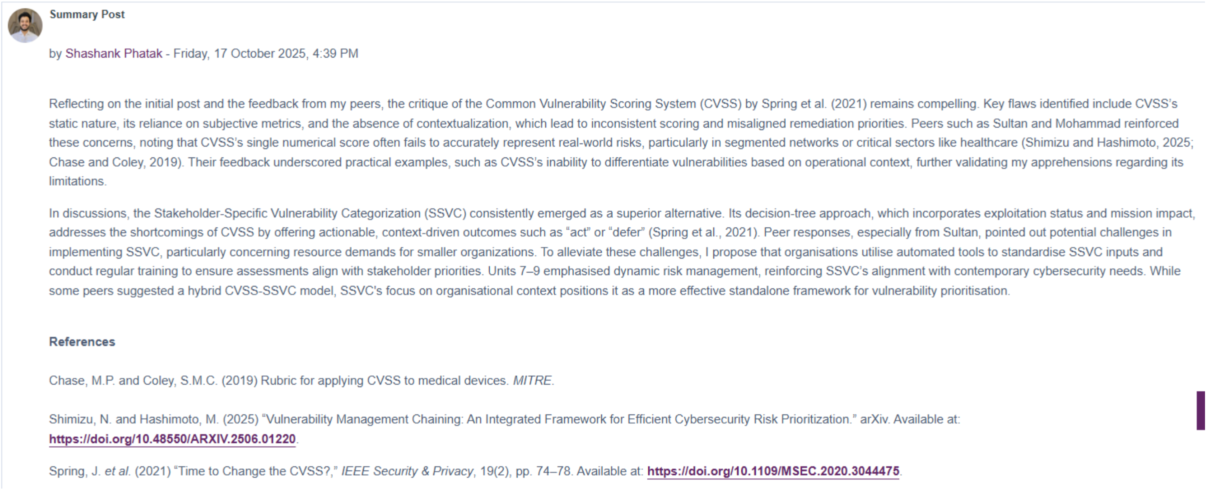
Allodi, L. and Massacci, F. (2014) "Comparing Vulnerability Severity and Exploits Using Case-Control Studies," *ACM Transactions on Information and System Security*, 17(1), pp. 1–20. Available at: **https://doi.org/10.1145/2630069**.

Endor Labs (2024) CVE, EPSS, SSVC, and VEX: prioritising vulnerabilities at scale. Available from: **https://www.endorlabs.com/learn/cve-vulnerability-epss-ssvc-reachability-vex** [Accessed: 27 September 2025].

Ghanem, T., et al. (2025) Evaluating vulnerability prioritisation frameworks: CVSS, EPSS and SSVC in large-scale ecosystems. *arXiv preprint*. Available at: **https://arxiv.org/abs/2508.13644** [Accessed: 27 September 2025].

Spring, J. *et al.* (2021) "Time to Change the CVSS?," *IEEE Security & Privacy*, 19(2), pp. 74–78. Available at: **https://doi.org/10.1109/MSEC.2020.3044475**.

Summary Post



Summary Post

by Shashank Phatak - Friday, 17 October 2025, 4:39 PM

Reflecting on the initial post and the feedback from my peers, the critique of the Common Vulnerability Scoring System (CVSS) by Spring et al. (2021) remains compelling. Key flaws identified include CVSS's static nature, its reliance on subjective metrics, and the absence of contextualization, which lead to inconsistent scoring and misaligned remediation priorities. Peers such as Sultan and Mohammad reinforced these concerns, noting that CVSS's single numerical score often fails to accurately represent real-world risks, particularly in segmented networks or critical sectors like healthcare (Shimizu and Hashimoto, 2025; Chase and Coley, 2019). Their feedback underscored practical examples, such as CVSS's inability to differentiate vulnerabilities based on operational context, further validating my apprehensions regarding its limitations.

In discussions, the Stakeholder-Specific Vulnerability Categorization (SSVC) consistently emerged as a superior alternative. Its decision-tree approach, which incorporates exploitation status and mission impact, addresses the shortcomings of CVSS by offering actionable, context-driven outcomes such as "act" or "defer" (Spring et al., 2021). Peer responses, especially from Sultan, pointed out potential challenges in implementing SSVC, particularly concerning resource demands for smaller organizations. To alleviate these challenges, I propose that organisations utilise automated tools to standardise SSVC inputs and conduct regular training to ensure assessments align with stakeholder priorities. Units 7–9 emphasised dynamic risk management, reinforcing SSVC's alignment with contemporary cybersecurity needs. While some peers suggested a hybrid CVSS-SSVC model, SSVC's focus on organisational context positions it as a more effective standalone framework for vulnerability prioritisation.

References

Chase, M.P. and Coley, S.M.C. (2019) Rubric for applying CVSS to medical devices. *MITRE*.

Shimizu, N. and Hashimoto, M. (2025) "Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization." arXiv. Available at: **https://doi.org/10.48550/ARXIV.2506.01220**.

Spring, J. *et al.* (2021) "Time to Change the CVSS?," *IEEE Security & Privacy*, 19(2), pp. 74–78. Available at: **https://doi.org/10.1109/MSEC.2020.3044475**.