UNIT 8: COLLABORATIVE DISCUSSION 2 -PEER RESPONSE

[redacted]'s critique of CVSS aligns with literature in identifying its principal weaknesses: a focus on severity rather than risk, insufficient contextual sensitivity, and scoring inconsistency (Akbar, 2020; Spring et al., 2021a; Spring et al., 2021b; Howland, 2021; Wunder et al., 2024). This critique is further strengthened by drawing attention to attacker behaviour and exploit availability (Allodi and Massacci, 2014), supported by evidence that exploit likelihood signals enhance remediation outcomes (Romanosky et al., 2020). Indeed, CVSS is not suitable as a stand-alone tool for risk prioritisation (Howland, 2023), yet it retains value as a descriptive severity measure (Mell et al., 2022).

However, implementing SSVC is challenging due to several practical constraints. SSVC requires cross-departmental collaboration and is resource intensive, which may be unsustainable for less mature or smaller organisations (Dudley, 2022). Its stakeholder-specific design may reduce effectiveness in hybrid or overlapping roles (Bahar and Wazan, 2024). Furthermore, customisation of decision trees can distort decision processes and reduce effectiveness (Carnegie Mellon University, 2025). Moreover, as SSVC produces qualitative outputs (e.g., "defer," "schedule"), it avoids CVSS's arithmetic flaws but introduces subjectivity and limits integration with quantitative systems (Bahar and Wazan, 2024). Finally, differing stakeholder priorities can lead to divergent outcomes (Akbar, 2020).

Despite these limitations, combining SSVC with EPSS can improve prioritisation by incorporating exploit likelihood, enabling more efficient allocation of resources. However, EPSS accuracy depends on access to high-quality and timely data, which is not always assured (Romanosky et al., 2020).

Although SSVC offers transparency and stakeholder specificity, empirical research remains limited on effectiveness and alignment with established systems (Koscinski et al., 2025). Moreover, while SSVC excludes regulatory obligations (Spring et al., 2021b, p. 54), PCI DSS mandates the use of CVSS scoring, rendering CVSS unavoidable (PCI Security Standards Council, 2017, p.8; Singh Gusain, 2024; Shimizu and Hashimoto, 2025).
Hence, while [redacted]'s proposal is well-argued, compliance obligations and practical constraints suggest that SSVC should complement rather than replace CVSS.

References

Dudley, A. (2022) *What is SSVC (Stakeholder-Specific Vulnerability Categorization)?* Available at: https://nucleussec.com/blog/what-is-ssvc-stakeholder-specific-vulnerability-categorization/ (Accessed: 14 September 2025).

Akbar, M. (2020) *A critical first look at Stakeholder Specific Vulnerability Categorization (SSVC).* Available at: https://blog.secursive.com/posts/critical-look-stakeholder-specific-vulnerability-categorization-ssvc/ (Accessed: 17 September 2025).

Allodi, L. and Massacci, F. (2014) 'Comparing vulnerability severity and exploits using case-control studies', *ACM transactions on information and system security (TISSEC)*, 17(1), pp. 1-20. Available at: https://doi.org/10.1145/2660363 (Accessed: 17 September 2025).

Bahar, A. and Wazan, A.S. (2024) ‘On the validity of traditional vulnerability scoring systems for adversarial attacks against LLMs’. Available at: https://arxiv.org/abs/2412.20087 (Accessed: 26 August 2025).

Carnegie Mellon University (2025) *Modeling other decisions and customization guidance*. In: *SSVC: Stakeholder-specific vulnerability categorization – How-To guide*. CERT/CC. Available at: https://certcc.github.io/SSVC/howto/tree_customization/#customizing-for-risk-appetite (Accessed: 26 August 2025).

Howland, H. (2021) ‘CVSS: Ubiquitous and broken’, *Digital Threats: Research and Practice,* 4(1), pp. 1-12. Available at: https://doi.org/10.1145/3491263 (Accessed: 26 August 2025)

Koscinski, V., Nelson, M., Okutan, A., Falso, R. and Mirakhorli, M. (2025) ‘Conflicting Scores, confusing Signals: an empirical study of vulnerability scoring system*s’.* Available at: https://arxiv.org/abs/2508.13644 (Accessed: 28 August 2025).

PCI Security Standards Council (2017) *Information supplement: Penetration testing guidance.* Available at: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf (Accessed: 29 May 2025).

Romanosky, S., Edwards, B., Jacobs, J. and Roytman, M. (2020) ‘Measuring the cost-effectiveness of vulnerability remediation’, *Proceedings of the Workshop on the Economics of Information Security (WEIS 2020)*, Brussels, Belgium, pp. 1–22. Available at: https://arxiv.org/pdf/1908.04856 (Accessed: 17 September 2025).

Singh Gusain, V. (2024) *A hybrid approach to generate severity scores for prioritization of vulnerabilities*. Available at: https://norma.ncirl.ie/8319/1/vivekgusain.pdf (Accessed: 16 September 2025).

Shimizu, N. and Hashimoto, M. (2025) ‘Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization’. Available at: https://arxiv.org/abs/2506.01220 (Accessed: 17 September 2025).

Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D. (2021a) ‘Time to Change the CVSS?’, *IEEE Security & Privacy*, 19(2), pp.74–78. Available at: https://doi.org/10.1109/msec.2020.3044475 (Accessed 26 August 2025).

Spring, J., Householder, A., Hatleback, E., Manion, A., Oliver, M., Sarvapalli, V., Tyzenhaus, L., Yarbrough, C. (2021b) ‘Prioritizing vulnerability response: a stakeholder-specific vulnerability categorization (version 2.0)’. Available at: https://www.sei.cmu.edu/documents/606/2021_019_001_653461.pdf (Accessed 26 August 2025).

Wunder, M., Gutzmann, T., Wiesmaier, A. and Lipps, C. (2024) ‘Shedding light on CVSS: An empirical analysis of user scoring behaviour’, *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 1102-1121. Available at: https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00058 (Accessed: 26 August 2025).

Tutor feedback

None received