Peer Response 2 – Unit 7

Thank you, S,

Your post gives a clear overview of the weaknesses highlighted by Wunder et al. (2024), especially the inconsistency in how evaluators interpret metrics such as Scope and User Interaction. I agree that much of this comes from unclear metric definitions, and this has also been observed in studies involving experienced analysts (Holm and Afridi, 2015). You also make an important point about configuration weaknesses, since they often appear in practice but do not fit into the CVSS structure.

I also discussed SSVC in my own initial post, and I agree that its decision-tree structure removes much of the interpretive uncertainty found in CVSS. One slight nuance I would add is that SSVC relies heavily on reliable information about factors such as exploitation status and mission impact. When that information is incomplete, the decision tree can still lead to different outcomes. So, while SSVC is a strong alternative, it also has practical limits that organisations need to keep in mind.

While I have not found any published work that explicitly describes a hybrid model combining CVSS and SSVC, using the two together could help address some of the inconsistencies highlighted by Wunder et al. (2024).

How do you think SSVC performs when organisations do not have reliable information about exploitation status or mission impact?

References

Holm, H. and Afridi, K.K., 2015. An expert-based investigation of the Common Vulnerability Scoring System. Computers & Security, 53, pp. 18–30.

Wunder, J., Kurtz, A., Eichenmüller, C., Gassmann, F. and Benenson, Z. (2024) Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. Available at: https://arxiv.org/abs/2404.05955 (Accessed: 5 December 2025).