Peer Response 1

Thank you, A

I found your points well-structured and easy to follow. You clearly explain the main issue raised by Wunder et al. (2024), especially the inconsistency in how evaluators interpret and apply core CVSS metrics such as Attack Vector and User Interaction. Your point about organisations using CVSS as a direct risk measure, even though the specification warns against this, highlights a common gap between how the framework is intended to be used and how it is applied in practice.

Your discussion of EPSS as an alternative made me look into it further, and I agree that it has some real strengths. What stood out to me was that EPSS provides an empirical estimate of the likelihood of exploitation, whereas CVSS does not. Because EPSS outputs a probability, it can also be used in methods such as Monte Carlo simulations. Since we have been working with Monte Carlo approaches in this module, it was interesting to see how EPSS fits naturally into uncertainty and probability models rather than into fixed scores. This makes the method more dynamic and better at reflecting changes over time.

A hybrid approach could also help address the inconsistency highlighted by Wunder et al. (2024). In this model, CVSS provides technical context, while EPSS indicates which vulnerabilities should be prioritised. Analyses from FIRST show that EPSS reduces both

false positives and false negatives compared with relying solely on CVSS (FIRST, 2023). This allows mitigation efforts to focus on vulnerabilities more likely to be exploited, while CVSS remains helpful in understanding their characteristics.

A question I had was how reliable you think EPSS is when exploit data is very limited?

References

Cheimonidis, P. and Rantos, K. (2025) ‘A proactive and time-sensitive cyber risk assessment model integrating Markov chains and Bayesian networks’, IEEE Access, 13, pp. 96911–96932

FIRST EPSS SIG (2023) Exploit Prediction Scoring System (EPSS): Technical Documentation. Available at: https://www.first.org/epss
(Accessed: 6 December 2025).
.

Wunder, J. et al. (2024) Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. arXiv.org.Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2858809873 [Accessed 7 December 2025]