Summary Post – Unit 9

This discussion changed how I understood the role of CVSS within vulnerability management. In my initial post, I focused on the empirical critique presented by Wunder et al. (2024), which shows that CVSS scores are often inconsistent across evaluators and can even change for the same evaluator over time. Metrics such as User Interaction and Scope are applied inconsistently in practice, weakening the reliability of the final score. Feedback from peers supported my assessment that these inconsistencies occur in practice.

I agree with this critique, both from the literature and from practice. Empirical studies show that CVSS scoring is influenced by interpretation, and that slight differences in scoring can affect prioritisation outcomes (Allodi et al., 2020; Holm and Afridi, 2015). Peer feedback further supported that CVSS is most useful as a preliminary tool, particularly in agile environments where quick categorisation is needed.

One Key learning outcome for me was that CVSS should not be used in isolation. On its own, it provides information about technical severity, but not about likelihood or context. Through the module content and peer discussion, I learned that CVSS provides greater reliability when used alongside a quantitative approach, where severity can be combined with other factors to support prioritisation rather than replace it.

Among the alternatives discussed, SSVC represents a stronger option at the decision stage. SSVC focuses on guiding response actions rather than producing numerical severity scores. This reduces ambiguity and supports more consistent prioritisation by taking factors such as exploitation status, impact, and organisational priorities into account, rather than relying solely on severity.

Overall, this discussion helped me move from seeing vulnerability scoring as an endpoint to treating it as one input in a broader risk management process. CVSS remains useful for early assessment, but the combination of peer feedback and module content clarified its limits and the need to combine it with other approaches when priorities are set.

References

Allodi, L., Cremonini, R., Massacci, F. and Shim, W., 2020. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empirical Software Engineering, 25(2), pp. 1063–1094.

Cybersecurity and Infrastructure Security Agency (CISA) (no date) Stakeholder-Specific Vulnerability Categorization (SSVC). Available at: https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc (Accessed: 17 December 2025).

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. et al. (2024) Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities.