Task ‘Collaborative Learning Discussion 2’ Unit 7

‘Initial Post’

The authors of "Shedding Light on CVSS Scoring Inconsistencies," criticize several characteristics of the Common Vulnerability Scoring System (CVSS). They find that CVSS scores lack inter-rater consistency and therefore tend to be very subjective, noting that professionals frequently assign different values for core metrics such as Attack Vector, Scope, and User Interaction. Their follow-up study revealed that 68% of participants had provided a very inconsistent rating, which was also inconsistent with their earlier ratings, indicating that the issue originates from the ambiguity in the CVSS metric definitions rather than user proficiency and demonstrating that such methods appear to involve a degree of subjective perception.

(Wunder et al., 2023)

I agree with this critique to some degree. CVSS is intended to capture key vulnerability characteristics and guide severity-based prioritization, but its scoring structure lacks contextual justification. The CVSS specification itself warns against using scores as direct measures of risk, yet major compliance bodies including the U.S. government and the PCI DSS explicitly promote this misuse. Even organizations following intended practices rely on unreliable outputs. Overall, the current CVSS version remains inadequate for both its stated purpose and as a risk proxy. (Spring et al., 2018)

Among the alternative approaches identified in similar studies, the Exploit Prediction Scoring System (EPSS) provides a strong candidate to supplement or replace CVSS in vulnerability-prioritization workflows. EPSS uses empirical, data-driven modeling to assess the probability that vulnerability will be exploited in real-world conditions. This directly addresses one of CVSS's central weaknesses, its focus on theoretical severity rather than identifying risk arising from integrating diverse data sources, including threat data and local asset-criticality information. In environments with many vulnerability disclosures, a probabilistic, evidence-based score helps prioritize threats. EPSS is a could be considered a more practical foundation for risk-informed vulnerability management.

(Jacobs et al., 2023).

In conclusion, several studies have demonstrated that each risk management practice and approach has its own strengths and weaknesses. This means that each method has its own limitations in terms of the case being used. Combining mixed set of techniques may assist produce a more effective and reliable risk results which in turn can better support decision-making across complex risk environments.

(Thekdi et al., 2025).

References

- Jacobs, J. et al. (2023) Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights. arXiv.org. Available at: https://**********.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2781017466 [Accessed 2 December 2025]
- Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D., (2021). Time to Change the CVSS? IEEE Security & Privacy, 19(2), pp.74-78
- Thekdi, S. & Aven, T. (2025) Evaluating risk analyst views on uncertainty and knowledge aspects for risk characterization approaches. Journal of risk research. [Online] 28 (8), 912–928. Available at: https://**********.com/permalink/44UOES_INST/o3t9un/cdi_informaworld_taylorfrancis_310_1080_13669877_2025_2553847 [Accessed 5 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://**********.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2858809873 [Accessed 2 December 2025]