**Summary Post**

In their critique, Spring et al. (2021) point out significant flaws in the Common Vulnerability Scoring System's (CVSS) present methodology, most notably the absence of clear empirical rationale when turning qualitative data into numerical risk scores. As a result, the system gives priority to technical severity while ignoring important operational and contextual aspects that affect how easily vulnerabilities can be exploited. Allodi and Massacci (2014) have observed that the practical risk management of CVSS is limited due to its frequent inconsistency with real-world exploitability. The criticism further emphasises CVSS's failure to take into consideration the material effects of exploits, including their effects on availability, secrecy, and integrity.

Previous research, like Houmb et al. (2010), supports this observation by arguing for a more thorough risk assessment strategy that considers elements like impact frequency and real-world implications instead of concentrating just on technical features. By doing this, businesses are better able to rank vulnerabilities according to real dangers as opposed to arbitrary metrics.

A more context-sensitive methodology is provided by Spring et al. (2021) Stakeholder-Specific Vulnerability Categorisation (SSVC) as an alternative. By enabling businesses to customise risk assessments to their operational settings, SSVC guarantees that decisions about vulnerability management are founded on relevance and possible outcomes. This method improves decision-making and brings it closer to practical situations.

Peer review confirms the usefulness of this approach, concurring that SSVC offers a more flexible and practical framework for prioritising vulnerabilities. A flexible, context-based methodology has replaced static, technical scoring to better match the demands of current cybersecurity, where risk evaluation heavily depends on the operational context.

**References**  
Allodi, L. & 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.

Houmb, S.H., Franqueira, V.N.L. & Engum, E.A. (2010). Quantifying security risk level from CVSS estimates of frequency and impact. *Journal of Systems and Software*, 83(9), pp. 1622-1634.

Spring, J.M., Hatleback, E., Manion, A. & Shick, A. (2021). On the inadequacy of CVSS: A systematic study. *IEEE Security & Privacy*, 19(2), pp. 74-78.