**Peer Response 1**

To address the limitations of the Common Vulnerability Scoring System (CVSS) as outlined by Spring et al. (2021), several preventive measures could have been implemented. These measures aim to improve vulnerability management systems by making them more adaptable, context-aware, and responsive to dynamic threat environments.

Firstly, the integration of real-time exploitability data would significantly enhance the relevance of vulnerability scores. As noted by Santana et al. (2024), incorporating real-world metrics such as the presence of active exploit codes would allow for more accurate risk prioritisation. This would mitigate the issue of CVSS’s static nature, enabling organisations to respond to the most pressing threats based on current exploitability, rather than relying on generalised technical attributes.

Secondly, adopting a context-aware vulnerability scoring framework would better align vulnerability management with specific organisational needs. The Exploit Prediction Scoring System (EPSS), introduced by Spring et al. (2021), serves as a viable alternative to CVSS. EPSS focuses on the likelihood of exploitation by utilising historical data, which enhances its adaptability to evolving threat landscapes. This context-driven approach ensures that vulnerabilities are prioritised based on their real-world risk, thus addressing the skewed prioritisation inherent in CVSS.

Furthermore, implementing a continuous update and feedback mechanism would ensure that scoring models remain up to date with emerging vulnerabilities and attack patterns. This dynamic approach would allow organisations to adapt their defences in real-time, reflecting the latest threat intelligence.

Lastly, incorporating business impact considerations into vulnerability scoring would ensure that resource allocation is aligned with organisational priorities. By balancing technical severity with the potential impact on business operations, organisations can avoid over-prioritising vulnerabilities that pose minimal risk to critical systems.

In conclusion, these measures real-time data integration, context-aware frameworks, continuous updates, and business impact consideration—could address the limitations of CVSS, ultimately improving the effectiveness of vulnerability management.

References:

* Spring, J.M., Hatleback, E., Householder, A.D., Manion, A. and Shick, D. (2021) 'Time to change the CVSS?', *ResearchGate*.
* Santana, R. (2024) 'SecScore: A context-aware vulnerability scoring framework', *arXiv*.

**Peer Response 2**

To improve the efficacy of the Common Vulnerability Scoring System (CVSS) in giving precise risk assessments, several preventive actions should be put in place to overcome the constraints described by Spring et al. (2021):  
  
Justifiable and Transparent Scoring Formula: One major problem with the CVSS scoring formula is its lack of openness. The foundation of a scoring system should consist of well-defined and recorded concepts. Integrating modern algorithms like DistilBERT, as suggested by Costa et al. (2022), could enhance the relevance and comprehension of vulnerability scores by utilising natural language processing to more precisely comprehend vulnerability descriptions.

Contextual Information Incorporation: One of CVSS's main weaknesses is that it ignores contextual factors like the possibility of exploitation and the business impact. These elements could be added to CVSS to provide a more accurate and nuanced risk assessment. This restriction could be addressed by customising vulnerability assessments to organisational contexts and risk profiles through the use of a context-sensitive methodology such as Stakeholder-Specific Vulnerability Categorisation (SSVC) (Spring et al., 2021).

Separating Severity from danger: One of the main problems with the present CVSS architecture is that severity is sometimes mistaken for danger. To lessen this, it is crucial to develop unique measures for risk and severity, which will enable a more distinct differentiation between a vulnerability's technical attributes and possible operational consequences. The prediction accuracy of CVSS ratings would increase if risk indicators like exploit availability and system exposure were included (Howland, 2023).

Operational Flexibility: CVSS is less relevant in terms of operations due to its strict grading methodology in various organisational settings. To tackle this issue, it would be possible to enhance the flexibility of CVSS to suit various use cases. This would allow businesses to adjust scores according to their distinct operational contexts and threat environments (Spring et al., 2021).

Examining Material Consequences: The application of CVSS in real-world risk assessment is limited by its lack of emphasis on material consequences, such as operational or financial damage. To remedy this, the scoring system might incorporate effect assessments that are unique to a given firm, guaranteeing a thorough comprehension of the possible ramifications of a vulnerability.  
  
To sum up, by implementing these improvements, CVSS will become a much more dependable instrument for evaluating vulnerability risk and will be more in line with practical security requirements.

References:  
  
Costa, J.C., Roxo, T., Sequeiros, J.B.F., Proença, H. and Inácio, P.R.M. (2022) 'Predicting CVSS metric via description interpretation', *IEEE Access*, 10, pp. 59125-59134. DOI: 10.1109/ACCESS.2022.3179692.

Howland, H. (2023) 'CVSS: ubiquitous and broken', *Digital Threats: Research and Practice*, 4(1). DOI: 10.1145/3491263.

Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D. (2021) 'Time to change the CVSS?', *IEEE Security and Privacy*, 19(2), pp. 74–78. DOI: 10.1109/MSEC.2020.3044475.