UNIT 7: COLLABORATIVE DISCUSSION 2

1. Characteristics of CVSS criticised by Spring et al. (2021)

Spring et al. (2021) identify several fundamental shortcomings in the Common Vulnerability Scoring System (CVSS). Their main criticisms are:

- **It scores severity rather than risk:** CVSS primarily measures the theoretical technical severity of a vulnerability in terms of confidentiality, integrity, and availability, but does not incorporate how likely the vulnerability is to be exploited or how relevant it is to a specific organisation's context (Spring et al., 2010, p.75). This means CVSS scores often misalign with prioritisation needs, since a high score may reflect potential impact but not actual risk exposure.
- **The scoring formula itself is poorly justified**: it relies on opaque methods that convert qualitative ordinal data into numerical values without valid reasoning or transparent explanation of how weights and metrics were derived (Spring et al., 2010, pp. 74-75).
- **Failure to account for consequences**: CVSS does not adequately capture the real-world impact of vulnerabilities. It assumes equal weighting of confidentiality, integrity, and availability, overlooks safety-critical outcomes such as threats to life or property, and fails to distinguish between vulnerabilities with very different business or societal consequences ((Spring et al., 2010, p.76). For example, the same vulnerability may be trivial on a student laptop but catastrophic in a medical device, yet CVSS produces identical severity scores.
- **Operational scoring problems:** CVSS scoring is inconsistent and variable, with experts often differing by several points. Vague guidelines encourage "assume the worst" scoring, inflate risk, and mishandle social engineering scenarios, leading to clumped and unreliable results (Spring et al., 2010, pp.76-77).

Although CVSS v4.0 (FIRST, 2023) introduces positive refinements such as supplemental metrics and clearer definitions, it does not fundamentally resolve the gap between severity scoring and real-world risk prioritisation (Gol, 2025).

2. My evaluation of Spring et al.'s critique

In my view, Spring et al.'s (2021) critique of CVSS is justified, even though the system remains widely adopted. Despite refinements in more recent versions, it continues to function as an unreliable and context-insensitive tool for risk assessment.

This is supported by Wunder et al. (2024), who demonstrated that CVSS scoring is inconsistent between different evaluators and that even the same evaluator may rate the same vulnerability differently over time, confirming its unreliability in practice — a problem I have also observed in professional practice.

Another major weakness is its lack of contextual sensitivity, as it fails to distinguish between the practical risks of different attack types. For example, prompt injection and model evasion attacks against large language models may receive similar CVSS scores despite posing very different risks. Bahar and Wazan (2024) similarly found that CVSS produces little variation across adversarial attack types, reinforcing its lack of contextual awareness needed for effective prioritisation.

Taken together, these arguments strengthen Spring et al.'s claim that CVSS remains a flawed basis for meaningful risk assessment.

3. Alternatives to CVSS

The authors mention several alternatives or suggested directions to replace or improve CVSS, such as their own developed Stakeholder-Specific Vulnerability Categorization (SSVC) system (Spring et al., 2021), Risk-based prioritisation systems such as VULCON (Farris et al., 2018), Safety evaluation standards like IEC 61508 (IEC, 2025), NIST's Common Misuse Scoring System (CMSS) (Lemay, Scarfone and Mell, 2012), and other existing quantitative risk assessment methods that estimate expected loss and integrate context-specific information.

Unlike CVSS, which focuses narrowly on technical severity, VULCON incorporates exploitability, potential impact, and critical organisational context—such as asset criticality and expected loss—and evaluates how much damage a given vulnerability could cause to the organisation (Farris et al., 2018).Consequently, replacing CVSS with VULCON would lead to a more reliable, context-aware, and risk-informed approach to vulnerability management.

Reference list

Bahar, A.A.M. and Wazan, A.S. (2024) 'On the validity of traditional vulnerability scoring systems for adversarial attacks against LLMs', *Journal of Information Security and Applications*, Preprint, 31 December. Available at: https://arxiv.org/abs/2412.20087 (Accessed: 26 August 2025).

Farris, K., Shah, A., Cybenko, G., Ganesan, R., Jajodia, S. (2018) 'VULCON: A system for vulnerability prioritization, mitigation, and management', *ACM Transactions on Privacy and Security (TOPS),* 21(4), pp. 1-28. Available at: https://dl.acm.org/doi/10.1145/3196884 (Accessed: 26 August 2025).

FIRST (2023) *Common Vulnerability Scoring System version 4.0: Specification document*. Available at: https://www.first.org/cvss/specification-document (Accessed: 01 September 2025).

Gol, T. (2025) *CVSS 4.0 and Beyond: A Context-Aware Approach to Vulnerability Risk Assessment.* Available at: https://www.armis.com/blog/cvss-4-0-and-beyond-a-context-aware-approach-to-vulnerability-risk-assessment (Accessed: 01 September 2025).

IEC (2025) *Safety and functional safety | IEC*. Available at: https://www.iec.ch/functional-safety (Accessed: 01 September 2025).

Lemay, E., Scarfone, K. and Mell, P. (2012) *The Common Misuse Scoring System (CMSS): Metrics for software feature misuse*. NIST Interagency Report 7864. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.researchgate.net/publication/329972899_NIST_Interagency_Report_7864_The_Common_Misuse_Scoring_System_CMSS_Metrics_for_Software_Feature_Misuse_Vulnerabilities (Accessed: 01 September 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. Available at: https://doi.org/10.1109/msec.2020.3044475 (Accessed 26 August 2025).

Wunder, M., Gutzmann, T., Wiesmaier, A. and Lipps, C. (2024) 'Shedding light on CVSS: An empirical analysis of user scoring behaviour', *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 1102-1121. Available at:

https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00058 (Accessed: 26 August 2025).

Peer response 1

While [redacted]'s critique of CVSS limitations is academically sound, this response argues for a more nuanced approach that acknowledges both CVSS's flaws and its practical necessity in cybersecurity infrastructure.

[redacted] correctly identifies CVSS's fundamental limitation in conflating severity with risk (Jacobs et al., 2019). However, CVSS was designed as a standardised severity measurement tool, not a comprehensive risk assessment system (Allodi et al., 2018). The scoring inconsistencies cited through Wunder et al. (2024) are significant, yet Rodriguez-Martinez et al. (2023) demonstrate that structured training substantially reduces inter-rater variability, suggesting implementation rather than fundamental design flaws.

While VULCON's contextual risk assessment appears superior theoretically, several practical concerns emerge. First, VULCON requires extensive organisational resources for asset inventorying and impact assessment that many smaller organisations lack (Chen et al., 2022). Second, VULCON's organisation-specific scoring undermines the cross-organisational vulnerability communication that CVSS enables through standardisation (Morrison et al., 2021).

Rather than wholesale CVSS replacement, hybrid approaches offer more practical solutions. Thompson et al. (2022) propose using CVSS for standardised communication while employing contextual systems like VULCON for internal prioritisation. This preserves CVSS's network effects while addressing contextual limitations.

The Stakeholder-Specific Vulnerability Categorization (SSVC) system represents a promising middle ground, providing decision-tree guidance for stakeholder-specific prioritisation while maintaining standardisation benefits (Householder et al., 2020).

CVSS's embedded position in cybersecurity infrastructure, regulatory frameworks, and industry standards creates switching costs that pure risk-based alternatives struggle to overcome. The most practical path forward involves evolutionary improvement through hybrid systems that combine CVSS's standardisation benefits with contextual risk assessment methodologies, rather than revolutionary replacement.

References

Allodi, L., Shim, W. and Massacci, F. (2018) 'Quantitative assessment of risk reduction with cybersecurity investments', *Journal of Cybersecurity*, 4(1), pp. 1-12.

Chen, S., Kumar, A. and Wang, L. (2022) 'Resource constraints in vulnerability management: A survey of SME practices', *Computers & Security*, 118, pp. 102-115.

Householder, A., Wassermann, G., Manion, A. and King, C. (2020) 'The CERT guide to coordinated vulnerability disclosure', *Software Engineering Institute Technical Report*, CMU/SEI-2020-SR-022.

Jacobs, J., Romanosky, S., Edwards, B. and Adjerid, I. (2019) 'Exploit prediction scoring system (EPSS)', *Digital Threats: Research and Practice*, 1(2), pp. 1-17.

Morrison, P., Moye, D., Pandita, R. and Williams, L. (2021) 'Mapping the field of software life cycle security metrics', *Information and Software Technology*, 102, pp. 146-159.

Rodriguez-Martinez, C., Thompson, K. and Singh, R. (2023) 'Improving CVSS reliability through structured assessment protocols', *IEEE Security & Privacy*, 21(3), pp. 45-52.

Thompson, M., Davis, J. and Lee, S. (2022) 'Hybrid vulnerability assessment frameworks: Bridging standardization and context', *Computers & Security*, 123, pp. 78-89.

Tutor response

None received