UNIT 9: COLLABORATIVE DISCUSSION 2 -SUMMARY

The discussion has demonstrated broad agreement on the inherent limitations of CVSS and has highlighted the comparative advantages of alternative approaches.

All contributors recognise CVSS's weaknesses: it measures severity rather than risk, relies on an opaque formula, overlooks real-world consequences, and yields inconsistent results (Spring et al., 2010; Wunder et al., 2024). Notwithstanding its limitations, CVSS remains difficult to replace, as standards such as NIST (2022) and PCI DSS (PCI Security Standards Council, 2017) require vulnerability assessments using CVE and NVD data, both of which apply CVSS scoring. This reliance renders CVSS a de facto requirement.
CVSS v4.0 (FIRST, 2023) introduces refinements but fails to address the gap between severity scoring and real-world risk prioritisation (Gol, 2025).

The alternative frameworks discussed each mitigate specific weaknesses of CVSS but also introduce their own challenges:

- EPSS offers predictive value but relies on timely, high-quality data, which is not always assured (Romanosky et al., 2020). Like CVSS, it remains insufficient for addressing AI vulnerabilities, as it depends on CVE and NVD data, that do not capture AI-specific threats (Jacobs et al., 2021)

- SSVC enhances decision-making but is resource-intensive and organisationally complex, particularly for smaller organisations (Dudley, 2022). Additionally, its qualitative outputs add subjectivity, complicate integration with quantitative systems, and may yield divergent outcomes where stakeholder priorities differ (Bahar and Wazan, 2024; Akbar, 2020; Carnegie Mellon University, 2025).

- VULCON offers superior context-specific assessment but is resource-intensive (Farris et al., 2018). Its organisation-specific scoring enhances internal prioritisation but undermines cross-organisational comparability.

Empirical comparison of CVSS, SSVC and EPSS reveals significant disparities in vulnerability rankings, affecting prioritisation (Koscinksi et al., 2025). Moreover, automation is essential: EPSS requires it to maintain predictive accuracy through continuously updated threat data, while SSVC depends on it to reduce resource intensity and enable consistent, scalable application.

Saheed's proposed hybrid approach presents an improvement by overcoming the limitations of CVSS. However, combining multiple systems introduces additional limitations and complexity, underscoring the need for more transparent, consistent and operationally aligned models.

Reference list

Akbar, M. (2020) *A critical first look at Stakeholder Specific Vulnerability Categorization (SSVC).* Available at: https://blog.secursive.com/posts/critical-look-stakeholder-specific-vulnerability-categorization-ssvc/

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).

Carnegie Mellon University (2025) *Modeling other decisions and customization guidance*. In: *SSVC: Stakeholder-specific vulnerability categorization – How-To guide*. CERT/CC. Available at: https://certcc.github.io/SSVC/howto/tree_customization/#customizing-for-risk-appetite (Accessed: 26 August 2025).

Dudley, A. (2022) *What is SSVC (Stakeholder-Specific Vulnerability Categorization)?* Available at: https://nucleussec.com/blog/what-is-ssvc-stakeholder-specific-vulnerability-categorization/ (Accessed: 14 September 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).

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).

Jacobs, J., Romanosky, S., Edwards, B., Roytman, M. and Adjerid, I. (2021) 'Exploit prediction scoring system (EPSS)', *Digital Threats: Research and Practice*, 2(3), pp.1–17. Available at: https://dl.acm.org/doi/pdf/10.1145/3436242 (Accessed:

Koscinski, V., Nelson, M., Okutan, A., Falso, R. and Mirakhorli, M. (2025) *Conflicting Scores, Confusing Signals: An Empirical Study of Vulnerability Scoring Systems*. Available at: https://arxiv.org/html/2508.13644v1 (Accessed: 23 September 2025).

NIST (2022) *NVD - Vulnerability Metrics*. Available at: https://nvd.nist.gov/vuln-metrics/cvss (Accessed:

OWASP Foundation (2025) *OWASP AI Vulnerability Scoring System (AIVSS).* Available at: https://aivss.owasp.org/ (Accessed:

PCI Security Standards Council (2017) *Information supplement: Penetration testing guidance.* Available at: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf (Accessed: 29 May 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).

Tutor feedback

None received