Collaborative Discussion 2 – CVSS – Summary Post

1. Summary Post

Discussion of the Spring et al. (2021) article on CVSS weaknesses and alternatives achieved broad consensus that CVSS displays several weaknesses that make it inappropriate for use as a standalone system, whilst opinion on a suitable replacement was split.

Noted weaknesses by all commenters were lack of context in analysis and inconsistent scoring, with studies by Allodi et al. (2018) and Aggarwal (2023) frequently cited.

The most common suggestion to address the weaknesses of CVSS was to use SSVC as a replacement; with its use of stakeholder specific decision trees praised for increasing context-based evaluation.

In response to these commenters CVSS's links to NIST and PCI DSS were mentioned, a practicality that makes wholesale replacement unrealistic.

My initial post analysed CVSS v.4.0, introduced after Spring et al's article. v.40 added metrics that include environmental factors, adding context to the vulnerability severity score (FIRST, 2023). I then proposed combining CVSS v.4.0 with EPSS, an exploit scoring system (FIRST, 2025).

In response to my suggestion, both Mohammed and Miriam pointed out that these systems require users to have some familiarity with the scoring system to optimise use. This point is backed by research by Aggarwal (2023) and Tan (2025).

These responses, combined with my initial post's conclusion that v.4.0 does not fundamentally change the usability issues of CVSS, made Omar's suggestion to utilise this combination for patch management extremely strong.

Given the entirety of the discussion a more suitable overall solution would be to combine all three systems. CVSS for a severity rating and some environmental context, EPSS for exploit likelihood, and SSVC for user friendly and qualitative decision making.

2. References

Allodi et al. (2018) 'The effect of security education and expertise on security assessments: The case of software vulnerabilities'. *Workshop on the Economics of Information Security (WEIS)*, Innsbruck, Austria, 18–19 June. Available at: https://doi.org/10.48550/arXiv.1808.06547

Aggarwal, M. (2023) 'A Study of CVSS v4.0: A CVE Scoring System', *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Gautam Buddha Nagar, India. Pp. 1180-1186. Available at: https://doi.org/10.1109/IC3I59117.2023.10397701

FIRST. (2023) *Common Vulnerability Scoring System version 4.0; Specification Document*. Available at: https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf (Accessed 12 September 2025).

FIRST. (2025) *EPSS: Exploit Prediction Scoring System*. Available at: https://www.first.org/epss/ (Accessed 11 September 2025).

Spring et al. (2021) 'Time to Change the CVSS', *IEEE Security & Privacy*, 19(2), pp. 74-78. Available at: https://doi.org/10.1109/MSEC.2020.3044475

Tan et al. (2025) 'Analysis of Vulnerability Severity and Exploit Probability Scoring Frameworks: CVSS and EPSS', *2025 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA. Pp. 54-59. Available at: https://doi.org/10.1109/SIEDS65500.2025.11021216