Collaborative Discussion Post 2 – CVSS – Responses to Peers

1. Response to Mohammed Alnuaimi

Mohammed's initial post accurately describes the issue of using CVSS to analyse the severity of vulnerabilities and designing an organisational security strategy for dealing with them. Due to its inability to incorporate context it cannot give a complete view of a vulnerability.

It is worth noting that there is a secondary issue: CVSS being used as a de-facto risk analysis tool (Spring et al., 2021), something that it is not designed for (FIRST, 2015), and not capable of being (Howland, 2022).

Mohammed's reasoning for proposing SSVC as a suitable replacement for CVSS is logical. However, although he mentions that CVSS is widely employed, this idea could be analysed deeper to reach the conclusion that CVSS is too embedded into security organisational culture to be replaced completely. Several important organisations require or promote CVSS use (NIST, no date; PCI, 2015).

Therefore, a combination of SSVC and CVSS would be a more suitable solution. CVSS can be used to establish a baseline severity for a particular vulnerability, and then SSVC can be used add context, helping to prioritise the response of a specific company.

The best solution would be to go a step further and incorporate the Exploit Prediction Scoring System (EPSS). EPSS uses real-world data to rank the likelihood of vulnerabilities being exploited in the immediate future (FIRST, 2025). Use of this trifecta allows both multi-faceted data driven, and context led decision making to be applied.

References

FIRST. (2015) *Common Vulnerability User Guide v3.0; User Guide.* Available at: https://www.first.org/cvss/v3-0/cvss-v30-user_guide_v1.6.pdf (Accessed 11 September 2025).

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

Howland, H. (2022) 'CVSS: Ubiquitous and Broken', *Digital Threats: Research and Practice*, 4(1), pp. 1-12. Available at: https://doi.org/10.1145/3491263

NIST. (no date) *National Vulnerability Database: Common Vulnerability Scoring System Calculator.* Available at: https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator (Accessed 12 September 2025).

PCI Security Standards Council. (2015) *PCI DSS Quick Reference Guide*. Available at: https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (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

2. Response to Omar

Your post gives a detailed explanation of the problems with CVSS discussed by Spring et al. (2021). Your summary of the system as misleading and lacking practicality for real-world use was an excellent point and is supported by Howland (2022), who states the system can actually compromise security.

It then makes sense that you would advocate for the replacement of CVSS, in favour of SSVC, for its flexibility and ease of use. However, in practical terms CVSS cannot be replaced outright as its is too widely used in core systems and standards, such as the NVD and PCI DSS (NIST, no date; PCI, 2015).

A combination of systems and frameworks would be more likely to be adopted.

Approach 1 is to combine CVSS, SSVC and EPSS. This would bring together a vulnerability severity score from CVSS (FIRST, 2019), the context-based decision-making of SSVC (Spring et al, 2021), and data backed analysis of exploitation likelihood from EPSS (FIRST, 2025).

Approach 2 uses CVSS v4.0, introduced after the article from Spring et al. (2021) was published. v4.0 introduces measures that move towards a more practical approach, alongside the original severity score. These include allowing modifications to base metrics to take organisational environments into account and supplemental metrics for more context (FIRST, 2023). The changes theoretically make SSVC unnecessary, thus CVSS v4.0 could be combined solely with EPSS for a workable system.

References

FIRST. (2019) *Common Vulnerability User Guide v3.1; User Guide*. Available at: https://www.first.org/cvss/v3-1/user-guide (Accessed 12 September 2025).

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).

Howland, H. (2022) ‘CVSS: Ubiquitous and Broken’, *Digital Threats: Research and Practice*, 4(1), pp. 1-12. Available at: https://doi.org/10.1145/3491263

NIST. (no date) *National Vulnerability Database: Common Vulnerability Scoring System Calculator.* Available at: https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator (Accessed 12 September 2025).

PCI Security Standards Council. (2015) *PCI DSS Quick Reference Guide.* Available at: https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (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