# The Challenges of CVSS And Its Possible Alternatives

## Initial Post

In this age and generations in various societies across the globe, many people show massive knowledge in cybersecurity, which is why it is vital that all organisations using technological devices have solid contingencies in place, in the event of foreign, software, or malware attacks (Balsam et al., 2025, p. 1). That is why the Common Vulnerability Score System (CVSS) came into use. Even though many organisations and businesses have been using CVSS, some researchers have intensely critiqued its qualities and proceeded to provide better alternatives for the system. According to Spring et al. (2021, p. 75), the system does not offer sufficient transparency when it comes to its formula method and how to arrive at the scores. They proceed to argue that a system as sensitive as that should offer high levels of transparency to enable other parties to spot any existing flaws and possibly counter them. In relation to Howard (2023, p. 3), I indeed agree with the authors because cyber-attacks have significantly increased over the years, and users of such systems need to be sure that the contingency they have in place is working and can be easily relied upon in the event of cyber danger.

Another characteristic the authors argue is a fault of the CVSS: its ability to only measure the intensity of a technical vulnerability, and its inability to show the risk associated with the vulnerability (Spring et al., 2025, p. 75). Surely, when organisations often use technical devices during their operations, it is definitely a critical need of theirs to make sure they understand the risk of using such devices, which then helps them find the solutions they may turn to when the risk becomes a present problem. Undeniably, the CVSS plays a crucial role in assisting those organisations in measuring the levels of various vulnerabilities. Regardless, it lacks the capacity to measure the risks those vulnerabilities may cause. Thus, ensuring one’s technical security system aligns with aspects such as the IEC 61508 Standard, which provides the criteria that a security system, such as CVSS, should offer and cover (Fowler, 2022, p. 10). This critique is a crucial point the authors make, and I support it because I believe a system such as CVSS should not only measure vulnerabilities but also show the risks involved, so that parties engaging with technical devices may adequately prepare for challenges that may arise in the near future.

Aside from critiquing CVSS and its inability, from the alternatives they provide, I firmly believe the Stakeholder-Specific Vulnerability Categorization (SSVC) is better because it primarily covers the number one and critical area CVSS fails at, which is assessing the risk of vulnerability scores across various areas (Koscinski, 2025, p. 3; Spring et al., 2025, p. 3). Its Tree-based formula and concept help users and organisations determine how a particular vulnerable area or aspect poses risks to their operations, and they can get ahead of the consequences those risks may bring. Therefore, SSVC is a good alternative, but it can be improved when compared with the IEC 61508 Standard to determine whether it correctly identifies risks that may arise.

## References

Balsam, A., Walkowski, M., Nowak, M., Oko, J. and Sujecki, S., 2025. Automatic CVSS-Based Vulnerability Prioritization and Response with Context Information and Machine Learning. Applied Sciences, 15(16), p.8787. https://www.mdpi.com/2076-3417/15/16/8787

Fowler, D., 2022. IEC 61508 viewpoint on system safety in the transport sector: Part 1–An overview of IEC 61508. Safety-Critical Systems EJournal, 1(2). https://scsc.uk/journal/index.php/scsj/article/view/13

Howland, H., 2023. CVSS: Ubiquitous and broken. Digital Threats: Research and Practice, 4(1), pp.1-12. https://dl.acm.org/doi/abs/10.1145/3491263

Koscinski, V., Nelson, M., Okutan, A., Falso, R., and Mirakhorli, M., 2025. Conflicting Scores, Confusing Signals: An Empirical Study of Vulnerability Scoring Systems. arXiv preprint arXiv:2508.13644. https://arxiv.org/abs/2508.13644

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. https://ieeexplore.ieee.org/abstract/document/9382369/

Spring, J.M., Householder, A., Hatleback, E., Manion, A., Oliver, M., Sarvapalli, V., Tyzenhaus, L., and Yarbrough, C., 2021. Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization (version 2.0). Software Engineering Institute (SEI), Tech. Rep. https://www.sei.cmu.edu/library/file_redirect/2021_019_001_653461.pdf/

### Peer Posts

#### *Peer Response 1*

Similar to my interaction and perspective of the primary article under discussion, Shashank also strongly agrees that the CVSS has indeed helped in the past, but it leaves a significant room for severe consequences in the event of software, malware, and other forms of cyber-attacks, since it does not show the potential of the risks the vulnerability scores pose to users. Therefore, both of us, as individuals with knowledge of how vulnerability and security systems should work, agree that CVSS does not offer sufficient safety to users and the ability for them to remain steps ahead of cyber-attacks and other technical malfunctions. Additionally, Shashank has conducted thorough research on the topic under discussion and has provided a detailed description of CVSS, as well as explored how SSVC can serve as a better alternative.

### *Peer Response 2*

Mohammad discusses the characteristics of SSVC and why it is a better replacement for the traditional CVSS. He does not just mention the alternative, but discuss it in depth, to show someone why system A, for instance, is good, but why B is better and should be adopted by everyone at risk of technical problems. The arrangement of this peer's work is simple and easily understandable, which is how a short response to an assignment should be. Additionally, his response is direct and to the point, free of any unnecessary information, which may otherwise reduce the magnitude of one's argument.

### Summary Post

As discussed earlier, a security system such as CVSS should offer more than just vulnerability scores. It is irrefutable that these vulnerability scores are essential, but they become "short-handed" because it does not efficiently show the risks of those vulnerabilities and how they can be mitigated. Therefore, SSVC becomes a better alternative because it addresses areas where CVSS is lacking and offers additional safety for individual's vulnerable to technical problems and attacks. Hence, as argued by the peers, it is essential to consider and implement this new model in new technical operations that require increased safety to prevent any unwanted consequences that may otherwise necessitate more extensive solutions. To avoid being blindsided, it is also important that users thoroughly examine the drawbacks of replacing CVSS with SSVC to ensure safety, as it may come with its own set of challenges.