Collaborative Learning Discussion 2

Initial Post

Wunder et al. (2024) point out several problems with the Common Vulnerability Scoring System. They show that different people often give very different scores for the same vulnerability, which suggests that CVSS is not applied consistently.

This inconsistency is evident in users' interpretations of several core CVSS metrics. Attack Vector, User Interaction and Scope are frequently applied differently by evaluators, even when they are working with identical information. Aksu et al. (2017) report that several CVSS metrics are loosely defined and difficult to apply consistently, even for trained analysts. This indicates that the definitions of these metrics leave too much room for interpretation, despite the formal descriptions provided in the CVSS v3.1 specification (FIRST, 2019), which makes it difficult for CVSS to provide reliable results.

I agree with most of the critique raised by Wunder et al. (2024), especially the point that several CVSS metrics are difficult to interpret consistently. Allodi et al. (2020) show that even experienced security professionals often disagree on how to score metrics such as User Interaction and Privileges Required, and that these differences can be significant enough to change the final severity rating. Holm and Afridi(2015) found similar patterns, with even experts placing the same vulnerability in different severity categories.
Even though the study identifies apparent weaknesses in how CVSS is interpreted and applied, I do not believe everything about the framework is negative. It continues to offer value as a quick and standardised first step in sorting vulnerabilities before more

detailed analysis is carried out, particularly in agile development environments where teams rely on rapid and consistent inputs during sprints.

The article mentions only one clear alternative to CVSS, namely SSVC, which the authors note uses decision trees to produce defined actions rather than numerical scores. This approach avoids many of the weaknesses in interpretations of the CVSS scoring system because evaluators follow a structured decision path rather than assigning values. Spring et al. (2021) also emphasise that SSVC is intentionally qualitative and focuses on the factors that organisations consider when making decisions, such as exploitation status, mission impact, safety implications, and system exposure. SSVC uses outcomes such as “Track”, “Attend”, or “Act”, so much of the ambiguity in CVSS is removed.

Considering the inconsistency demonstrated by Wunder et al., this framework offers a more reliable basis for vulnerability assessment and therefore represents a stronger alternative to CVSS.

References

Aksu, M.U., Dilek, M.H., Tatli, E.I., Bicakci, K., Dirik, H.I., Demirezen, M.U. and Aykir, T., 2017. A quantitative CVSS-based cybersecurity risk assessment methodology for IT systems. Proceedings of the International Carnahan Conference on Security Technology (ICCST), pp. 1–8. doi: 10.1109/CCST.2017.8167819.

Allodi, L., Cremonini, R., Massacci, F. and Shim, W., 2020. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empirical Software Engineering, 25(2), pp. 1063–1094.

FIRST, 2019. Common Vulnerability Scoring System v3.1: Specification Document. Available at: https://www.first.org/cvss/specification-document (Accessed: 4 December, 2025).

Holm, H. and Afridi, K.K., 2015. An expert-based investigation of the Common Vulnerability Scoring System. Computers & Security, 53, pp. 18–30.

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). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=640786 (Accessed: 5 December 2025).

Wunder. J. et al. (2024) Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities.