CVSS, according to its creators, offers a way to characterise vulnerabilities by reflecting their severity numerically from 0 to 10 (Spring et al.,2021, pg.74). This score can provide a baseline to do risk analysis for organisations and incident management teams as the potential impact of the vulnerability is documented according to the finding and according to Scarfone et al. 2009 the score is already in wide use in the information technology community.

However, Spring et al. (2021) challenged the scoring methodology, arguing that the CVSS v3.0 needs to be revised, as the technique mainly depicts only the system's possible technical severity. As it is more focused on technical seriousness, it misses accounting for the contextual situation of the organisation and the design. For example, a CVE-2022-22965 (NVD, 2022), which can aid attackers in carrying out our remote code execution, has a baseline score of 9.8 critical. However, more than this score is needed to determine the risk present in the company, as it could be that the application is isolated from the internet and is only available internally. In this case, the risk for this vulnerability will not be as significant as critical because it is not as readily available in the public space, and the critical score cannot be justified.

Despite these issues, CVSS is still an excellent reference for a risk assessment for an organisation or a particular system. Knowing the technical vulnerabilities is also a big part of the assessment. Still, several improvements can be made to this methodology, especially the scoring formula must be redone and justified for empirical justifications, and the scoring must be assessed using human studies(Spring J et al. 2021, pg. 76). Alternatively, using action categories instead of integers as the score is preferable (Spring J et al. 2021, pg. 76). This form of having actions would make the method more transparent and allows to differentiate risk of a system given the context. Due to the fact the action points can be carefully chosen according to the systems design and risk factors are better identified.

In conclusion, CVSS is an excellent baseline for assessing technical vulnerabilities. Yet, these scores should not be the only deciding factors when carrying out a risk assessment, as it misses crucial qualities like context evaluation of the system and intransparent formula. Therefore, these systems should be combined with other techniques to carry out risk assessments until an improved version of the CVSS is available.

References

NVD (2022) CVE-2022-22965. Available at: https://nvd.nist.gov/vuln/detail/cve-2022-22965 (Accessed: April 22, 2023).

Scarfone, K. and Mell, P., 2009, October. An analysis of CVSS version 2 vulnerability scoring. In 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 516-525). IEEE.

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.