Introduction

This article by Spring et al. (2021) and the entire collaborative discussion presented the opportunity to understand the Common Vulnerability Scoring System (CVSS) even better. The key for me is to understand the challenges of the CVSS score from Spring et al. (2021) point of view whilst combining it with my real-life experience and other authors' research. The aim is to prioritise and effectively use the CVSS while considering its challenges for vulnerability management.

The argument

A key point from this article is when the authors mentioned that CVSS was designed for how vulnerabilities affect traditional IT systems, with equal weighting to confidentiality, integrity, and availability. CIA can never weigh the same in every organisation. Every organisation must consider this when addressing risk and vulnerabilities as it is not one-size-fits-all and must not be equally weighted.

Threats can arise from misconfigurations and not only from narrowly defined vulnerabilities, which I agree with. This is evidenced in the OWASP top 10 where security misconfiguration is 8th on the list (OWASP, 2023). Therefore, if CVSS is not considering appropriate security hardening or improperly configured permissions in any given environment (i.e. cloud, on-prem, APIs etc.), then the industry has to reconsider CVSS as a compliance mechanism.

The Way Forward - the authors suggested that the new algorithm should address the various risk elements of context and material consequences (environmental scores, operational scoring problems, and material consequences). Transparency remains a rudimentary ask by the authors, adding that any replacement for CVSS should be accompanied by an empirical study of the consistency of robust human scoring that must be evaluated and explainable. The issue of contextual consideration/interpretation of values for each community and risk can not be overemphasised.

Conclusion

Finally, Njideka mentioned quantitative approaches as being more accurate and useful such as Monte Carlo Simulation, Bayes Theorem and Multi-Criteria Decision Analysis(MCDA) are good when talking about Risk Assessment tools, and might not exactly address vulnerability management as with CVSS. Ayo's mentioned 'Exploit Prediction Scoring System (EPSS) could be a good alternative especially because EPSS puts new technologies into consideration and tries to address CVSS's known flaws. EPSS is also interesting because it is governed by the Forum of Incident Response and Security Teams (FIRST) (Raza, M, 2023), which means continuous work is being done.

References

1. OWASP (2023). API8:2023 Security Misconfiguration. Available from: https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/ [Accessed October 13 2023].

2. Raza, M. (2023). The Exploit Prediction Scoring System (EPSS) Explained. Available from: https://www.splunk.com/en_us/blog/learn/epss-exploit-prediction-scoring-system [Accessed October 13 2023].

3. Spring, J., Hatleback, E. Householder, A. Manion, A. & Shick D. (2021-3). Time to Change the CVSS?. Available from: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=9382369 [Accessed October 9 2023].