Introduction

The authors of ‘Time to Change the CVSS?’, Spring et al. (2021) in their Editor's Note raised critical concerns regarding the Common Vulnerability Scoring System (CVSS). They posed indispensable questions regarding real-life applications while pointing out the lack of justification for the formula in risk assessment and decision-making. The authors’ criticisms provide valuable insights into the need for a more comprehensive and context-aware approach to vulnerability management.

The authors challenge the reliance on technical severity, pointing to the misalignment between technical details and broader risk concerns. This critique resonates with my on-the-job discussions with industry experts. Making it one of the most difficult topics to discuss and implement over the years. In my experience, I believe the CVSS represent the severity of a vulnerability, but does not reflect the risk that the vulnerability poses to an environment. The severity is not a holistic approach but focuses on a technical aspect of a service or application (Balbix, N.D.).

The authors argue that ‘ The assumption is that a more technically severe vulnerability is more important within an organization’s vulnerability prioritisation and risk mitigation processes (Spring et al, 2023).’ This should not always be the case, especially because risk appetite differs from one organisation to the other and different mapping can be applied by different communities.

The authors further question the effectiveness of alternative risk assessment methods compared to CVSS. Their concern about the practical utility of these alternatives is well-founded and also acknowledges the need for a method that suits the specific context. According to Singh & Joshi (2018) “Picking risk assessment model without investigation and examination, results in the implementation of security controls in the wrong places, wasting or misusing of resources and leaving an organization vulnerable to unanticipated threats”

The critique regarding the choice between quantitative and qualitative modeling is consistent with the need to select the most appropriate method based on the specific situation and data availability. Chester, J. (N.D.) in an article titled ‘A Closer Look at CVSS scores’ argued that CVSSv3.1 is a flawed scheme, stating that we can only hope for the next version to address various concerns.

Furthermore, the argument for replacing CVSS with "Stakeholder-Specific Vulnerability Categorization (SSVC)" is rooted in the pressing need for a more context-aware, flexible, and evidence-based approach to vulnerability assessment and risk management. SSVC addresses several critical shortcomings of CVSS;

- acknowledging the significant variability of vulnerabilities based on their specific environment.
- equips organizations to adapt their approach to suit their unique circumstances effectively.

It enables tailored assessments to fit specific industry needs.

Conclusion

Conclusively, I agree with the author's criticisms of CVSS and their call for a more comprehensive and context-aware approach to vulnerability management. Many cybersecurity experts acknowledge that the existing CVSS system is limited, and experience is what fills the gaps during vulnerability assessments (Osborne .C., 2023). Additionally, these critiques emphasize the need for a nuanced, multifaceted approach to risk assessment beyond technical severity. The authors therefore suggest that the way to fix this problem is to skip converting qualitative measurements to numbers.

References

1. Balbix (N.D.). What are CVSS Scores? Available from: https://www.balbix.com/insights/understanding-cvss-scores/ [Accessed October 10 2023].

2. Chester, J. (N.D.). A Closer Look at CVSS Scores. Available from: https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/. [Accessed October 10 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].