Changing the Common Vulnerability Scoring System

By

Jonathan Ajodo

It is now nearly hard for organisations to track and quickly fix vulnerabilities due to the rise in reported vulnerabilities annually. Hence, most organisations focus on the highest priority vulnerabilities based on the Common Vulnerability Scoring System (CVSS) to prioritise remediation efforts. However, Spring et al (2021) opined that the CVSS scoring algorithm is not justified, either formally or empirically. It was argued that the CVSS formula is not adequately justified because the qualitative responses to questions are converted to ordinal data and assign relative priority rankings which would not give an objective outcome. Spring et al (2021) further argued that CVSS scores severity, not security risk. According to Howland (2021), the lack of justification for the underlying formula and other limitations, the CVSS would not provide a meaningful metric for describing a vulnerability. I agree with this view. This more so that organisations appear to be interested in the risk that a vulnerability or flaw poses to them or how quickly they should react it.

Spring et al (2021) recommended the Stakeholder-Specific Vulnerability Categorization (SSVC) for prioritising vulnerabilities because it avoids the weaknesses in the CVSS. The SSVC aims to avoid one-size-fits-all solutions in favour of a modular decision-making system with clearly defined and tested parts that vulnerability managers can select and use as appropriate to their context (Spring, et al., 2021). The framework is focussed on decisions and the stakeholders making them rather than technical severity. The use of decision tree to prioritise vulnerabilities in SSVC addresses the lack of transparency in CVSS formula. Overall, vulnerability management involves several

stakeholders (with different objectives) prioritising vulnerabilities, as such, the CVSS with its inherent limitations is considered inadequate.

References

Howland, L. (2021). A Case Against CVSS: Vulnerability Management Done Wrong. Available from https://hlchowland.medium.com/a-case-against-cvss-vulnerability-management-done-wrong-99a0f8b740a3. [Assessed on 30 September 2022]

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021). Time to change the CVSS? IEEE Security & Privacy, 74-78.

Spring, J., Householder, A., Hatleback, E., Manion, A., Oliver, M., Sarvepalli, V., . . . Yarbrough, C. (2021). Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0). Available from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653459. [Assessed on 30 September 2022]