Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

Discussion 2: Summary Post

This discussion focused on the issues surrounding the use of the Common Vulnerability Scoring System (CVSS) when using it for risk management purposes. According to the views expressed by Spring et. al. (2021), a major problem with using CVSS for risk management is that it only considers the technical aspect, ignoring other factors such as context of the vulnerability or the consequences of successful exploitation.

For example, a vulnerability becomes more severe when it can be successfully exploited to gain control over a key asset system in a company. However, these contexts of vulnerabilities are ignored in CVSS (Spring et. al., 2021). This information is, however, very much relevant for risk management (Spring et. al., 2021). Other researchers, such as Tripiti and Singh (2013), agree on these views that the severity of a vulnerability depends on the context of the vulnerability, such as input sanitization and validation preventing the exploitation of a vulnerable library in a specific software tool.

Amrol Miah elaborated on the initial post, describing how CVSS 4.0, released in November 2023, included new metrics to calculate the severity of a vulnerability. Especially the context of a vulnerability is now considered more. Amrol explained that CVSS 4.0 includes metrics for the exploitability and impact of a vulnerability First.org (N.D.). Cipollone (2023) expands on this, stating other major advantages apart from better expression of the actual risk posed by the vulnerability compared to the older 3.1 standard are increased simplicity and clarity, as well as better adaptability and flexibility. For example, CVSS 4.0's modular structure allows for better adjustment of the scoring system to an organization's requirements (Cipollone, 2023). This especially was a criticism posed by Spring et. al. (2021), as the CVSS ignored organizational factors, such as in which system a vulnerability is present.

References

Cipollone, F. (2023) CVSS V4, what's new? What are the differences between CVSS 3.1 and 4. Available from: https://phoenix.security/cvss-v4-whats-new-and-how-does-it-differ-from-cvss-v3-1/ [Accessed 02 August 2024].

First.org (N.D.) CVSS v4.0 Specification Document. Available at: https://www.first.org/cvss/v4.0/specification-document [Accessed 1 August 2024].

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS? *IEEE Security & Privacy*, 19(2), pp.74–78.

Tripathi, A., Singh, U.K. (2013) Evaluation of severity index of vulnerability categories. International Journal of Information and Computer Security 5(4): 275-298. DOI: https://doi.org/10.1504/IJICS.2013.058211