Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

Discussion 2: Initial Post

CVSS, or Common Vulnerability Scoring System, presents a way to numerically identify the severity of a vulnerability (Spring et. al., 2021). The authors criticize just that CVSS only considers the technical severity of the vulnerability, not the actual security risk it causes (Spring et. al., 2021). According to Spring et. al. (2021), the formular for calculating the vulnerability score is unjustified given that it only rates the technical aspect of that specific vulnerability, ignoring factors such as the context and the consequences of the vulnerability (Spring et. al., 2021). Context, in this case, refers to factors such as if the vulnerability can even be exploited (and the extent to which it can be exploited) when it is present in shared libraries used by multiple tools (Spring et. al., 2021). In this case, factors such as whether the vulnerable library is present in a key asset system and how the system using the shared library is sanitizing inputs to the shared library need to be considered (Spring et. al., 2021). The consequences of successful exploitation are also relevant for risk management and not considered in CVSS, despite them being important for risk management (Spring et. al., 2021).

While the CVSS-score is relevant for identifying the individual vulnerability's severity, I agree that it shouldn't be used to assess the risk coming from that vulnerability for a specific business. This agrees with the views of Tripiti and Singh (2013), who argue that a vulnerability's severity is very much dependent on the existing mitigations for a specific vulnerability which are in place to prevent the vulnerability from being exploited.

The authors suggest using their own Stakeholder-Specific Vulnerability Categorization (SSVC) as an alternative (Spring et. al., 2021). SSVC helps assess the vulnerability's severity according to the environment in a specific organization (Waterfall, 2023). This helps eliminate one of the main critiques posed by Spring et. al. (2005).

References

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

Waterfall (2023) Stakeholder-Specific Vulnerability Categorization (SSVC) | Episode #102. Available from: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/stakeholder-specific-vulnerability-categorization-ssvc-episode-102/ [Accessed 27 July 2024].