[Units 7-9] Collaborative Learning Discussion 2: Summary Post

1. CVSS Critique

The Common Vulnerability Scoring System (CVSS), is a measurement of the severity of vulnerabilities, often quoted in qualitative risk analysis as a way to quantify qualitative risk. As qualitative risk analysis is considered subjective, CVSS is an unreliable measure of risk score by itself to take at face value (Spring et al., 2021; Spring et al., 2018).

A characteristic of CVSS discussed in Spring et al. (2021) is the assessment of a vulnerability's technical severity without situational context (Fruhwirth & Mannisto, 2009), not covering the risk it poses or indicating the recommended response time to the identified flaw in the system. It does not take into account time and environmental factors, which are operational influences. The authors deemed the CVSS does not have appropriate theoretical or empirical justification for the calculation and formula. Although it has ordered values by ranking, it is vague in the scale it uses. A common example in questionnaires is the Likert scale, with choices ranging from strongly agree to strongly disagree - the threshold between any two choices subjected to each individual's judgement, which leads to inconsistency in evaluating the quantified data at later stages. Spring et al. (2021) recommends changing the CVSS formula with proper empirical justification or creating a new system altogether which addresses the flaws of CVSS. Other qualitative scoring system alternatives to the CVSS include the Stakeholder-Specific Vulnerability Categorization (SSVC), Exploit Prediction Scoring System

(EPSS) and Vulnerability Priority Rating (VPR). The next section explores more about why SSVC would be a better alternative to CVSS.

2. SSVC as a CVSS Alternative

Established in 2019 through the collaboration of Carnegie Mellon University's Software Engineering Institute (SEI) and Cybersecurity and Infrastructure Security Agency (CISA), the Stakeholder-Specific Vulnerability Categorization (SSVC) is a more comprehensive alternative scoring system to the CVSS. As a guideline, SSVC aims to enable stakeholders to prioritise the next steps to respond to and manage a vulnerability (Spring et al., 2021). SSVC is a decision tree model which considers five elements: exploitation status, technical impact, ability to automate, mission prevalence and the impact on public well-being (CISA, N.D.). Based on these values, the model could arrive at any of the following four outcomes - track, track*, attend, and act. It is an improvement to SSVC as it provides more context in terms of time and environment, as well as empirical evidence in the evaluation process, setting a baseline for future works. SSVC is highly applicable in handling the prioritisation of remediation strategies in incidents involving vulnerabilities. Therefore, although more testing of the SSVC model would ensure its robustness, the SSVC scoring system is overall more holistic in comparison and could ultimately replace the CVSS as one of the mainstream risk analysis methods.

References

Cybersecurity and Infrastructure Security Agency (CISA). (N.D.) Stakeholder-specific vulnerability categorization. Available from: https://www.cisa.gov/ssvc [Accessed 22 November 2022].

Fruhwirth, C. & Mannisto, T. (2009) Improving CVSS-based vulnerability prioritization and response with context information. *3rd International Symposium on Empirical Software Engineering and Measurement.* Lake Buena Vista, 15-16 October. IEEE. 535-544.

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2018) Towards improving CVSS. *Software Engineering Institute.* Carnegie Mellon University.

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

Spring et al. (2021) Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0). *Software Engineering Institute.* Carnegie Mellon University.