In the publication Spring et al. (Spring et al. 2021) criticise and highlight a certain issue with the CVSS scoring pertaining to its lac of justification of the formula where; CVSS only prioritizes severity of a vulnerability based on its severity from a technical standpoint. Other notable issues, like lack of evidence for the formula constructions, derivation techniques and missing documentation of the ranking process.

I somewhat agree to the above statement and how the publication states about how CVSS is s severity centric scoring and completely ignores an organization’s context and exposure. To explain this let me draw upon a previous experience.

In a past penetration testing engagement, I had come across a couple of outdated operating system versions and some middleware technologies using deprecated versions of TLS [TLS1.0/1.1]. If put into context of CVSS the scoring for these vulnerabilities are in the high and critical ranges. However, if we include the organization context and exposure. The discovered vulnerabilities were a) completely internal, and b) accessible only if you had sufficient authentication and authorization to reach those areas, which are as of today not fully incorporated in the CVSS scoring. A TLS vulnerability is a “network” vulnerability which can be abused in an “unauthenticated” fashion as it is a Man-In-The-Middle Attack, but in this scenario, any case of leveraging the vulnerability in reality requires a lot of context.

The SSVC scoring considers important values like prevalence where it talks about how important a vulnerable component is within the asset, it also accounts for public well-being impact where it highlights on how the impact could serve on a broad sense (Physical, Environment, Financial, Psychological).

Spring, J., Hatleback, E., Householder, A., Manion, A., Shick, D., (2021). Time to Change the CVSS? Available at: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/9382369 [Accessed 29 September 2022].

CERT Coordination Center (CERT/CC) (2022). SSVC. GitHub. Available at: https://github.com/CERTCC/SSVC [Accessed 3 Oct. 2022].