**Initial Post**

by [Nkosana Mlambo](https://www.my-course.co.uk/user/view.php?id=16924&course=8751) - Thursday, 22 September 2022, 10:42 AM

Number of replies: 1

**Time to Change the CVSS?**

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity score to vulnerabilities, allowing responders to prioritise responses and resources according to threat. Scores are calculate based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. (Horváth et al, 2016).

In Spring et al (2021), the authors criticise several elements pertaining to CVSS, this includes its comprehensiveness, granularity, and robustness. In essence, the CVSS formula is not substantiated, and the scoring emphasises the technical severity of the vulnerability and not the actual security and business risk. The system therefore fails to account for technical and huma-organisational context, material consequences of the vulnerability, and provides inconsistent operational scoring.

Campagna (2020) states that enterprises need to measure risk, and they have been led to believe that CVSS scores can do that for them. The problem is that CVSS scores don’t measure risk. They measure the technical severity of a vulnerability.

Aboud (2020) further states that:

‘To be effective, security teams need to understand vulnerabilities in the context of business risk, and then use that data to prioritize their remediation efforts. By taking a risk-based approach to vulnerability management, security teams can focus on the vulnerabilities and assets that matter most, so they can address the organization’s true business risk instead of wasting their valuable time on vulnerabilities that have a low likelihood of being exploited’

It is imperative that businesses should focus on protecting their crown jewels when it comes to prioritization of risks, this includes the critical information assets and the impact, should the risk materialise. CVSS alone only prioritises the severity of the vulnerability and scores its exploitability with no focus on context and consequence e.g. A severe vulnerability observed on a non-critical system that will have no impact when exploited might be prioritised over a business-critical system with a moderate vulnerability that can cause harm to the business if exploited.

It makes more business sense to subscribe to a risk-based method and will yield more effective results as focus can be made more on concrete risks. The CVSS may lead organisations to focus on inaccurate vulnerabilities and cause an oversight on serious risks bearing devastating consequences.

Spring et al (2021) also suggest the Stakeholder-specific VulnerabilityCategorization(SSVC) as an alternative to CCVS.

SSVC is mostly a conceptual tool for vulnerability management. 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 (Hernández, 2022).

Therefore, SSVC is much more plausible to replace CVSS as it is more robust and risk-oriented, with the focus on tangible risks facing the organisation rather than focusing on vulnerabilities with the highest scores. CVSS merely provides the severity ratings of vulnerabilities and provides no context nor consequence of the risks posed by the vulnerabilities.

**References**

Horvath, A., Erdősi, P. & Kiss, F. (2016) *The Common Vulnerability Scoring System (CVSS) generations – usefulness and deficiencies*. Available from: https://core.ac.uk/display/200208052?utm\_source=pdf&utm\_medium=banner&utm\_campaign=pdf-decoration-v1 [Accessed 19 September 2022].

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) *Time to Change CVSS?.* IEEE Security & Privacy.

Campagna, R. (2020*) 5 Reasons to Stop Using CVSS Scores to Measure Risk*. Available from: https://www.balbix.com/blog/5-reasons-to-stop-using-cvss-scores-to-measure-risk/ [Accessed 19 September 2022].

Aboud, J. (2020) *Why You Need to Stop Using CVSS for Vulnerability Prioritization*. Tenable. Available from: https://www.tenable.com/blog/why-you-need-to-stop-using-cvss-for-vulnerability-prioritization [Accessed 21 September 2022].

Hernández , M. (2022) *Are vulnerability scores misleading you? Understanding CVSS score. Available from:* https://sysdig.com/blog/vulnerability-score-cvss-meaning/ [Accessed 21 September 2022].

Maximum rating: 👍 (1)

In reply to Nkosana Mlambo

**Re: Initial Post**

by [Doug Millward](https://www.my-course.co.uk/user/view.php?id=11298&course=8751) - Monday, 26 September 2022, 6:00 PM

Hi Nkosana  
a good post - but my question to you does CVSS even "measure the technical severity of a vulnerability?" What is the evidence for this? What is the background of the blog post(s) you quote? Why should you believe them? Spring et al is a single source as well - are they reliable? In my mind, these are important questions and as a master's student, you should be confident in your opinions and answers to them.