Re: Initial Post

by Ayo Adeniran - Tuesday, 10 October 2023, 6:04 PM

I agree with your assessment of the challenges identified in the article. The CVSS scoring formula is not transparent on how it is calculated, and the base score grouping element is not realistic because different vulnerabilities are based on different contexts of an event. According to FORTINET, CVSS scores represent the severity of a vulnerability, not the security risk that severity brings to a specific system.

I also agree with the mention of CVSS-Special Interest Group (SIG) and Quantitative Risk Analysis (QRA) frameworks as alternatives to bridge CVSS gaps. QRA applies to real-world problems, classifies risk according to likelihood and impact on a system, and makes it easier to determine which risk an organization should prioritize. QRA offers consistency, allows exploration of a range of options for addressing risk, reflects the degree of complexity, and provides means of analyzing the combined effect of risks rather than treating each risk separately

I agree with the explanation that Risk experts and consultants argue that quantitative approaches are more accurate and useful, and examples of such approaches include Monte Carlo Simulation, Bayes Theorem, and Multi-Criteria Decision Analysis (MCDA) 2.

In conclusion, I agree that a combination of more than one risk assessment framework can be used to address the challenges identified in the article.

Peer Response - Njideka

by Blessing Monsi - Friday, 13 October 2023, 5:10 PM

Hello Njideka,

Thank you for sharing your thoughts on Spring. et al. (2021) article, the author's argument is directed at the inadequacies of the Common Vulnerability Scoring System (CVSS), especially because the scoring focuses on the technical aspect of vulnerabilities without wholistically looking at other factors within a given environment. The review provides an insightful and well-structured analysis of the article's content.

As you have rightly pointed out, based on the article, the three areas or categories of challenges facing CVSS could help improve the use and implementation of CVSS across the industry.

You mentioned that CVSS does not handle the relationship between vulnerabilities as an independent scoring system can be misleading because vulnerabilities can be chained together, leveraging one to establish a precondition for another. This point can not be overemphasised, as I have had several real-life scenarios where clients ignored a particular patch management recommendation because several of their crucial systems rely on a vulnerable system, yet that system has several compensating controls.

Simply put, CVSS does not consider the compensating controls within an environment, this is a crucial flaw of the CVSS system and I hope the creators can assess this and find a way around resolving this.

To the best of my knowledge, based on CVSS 3.1, Spring et al (2021) point on 'Failure to account for consequence' might be in regards to the older CVSS as the latest ones consider the consequences of vulnerabilities.

"The Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component." (FIRST ORG., N.D.).

In conclusion, you summarised the challenges of CVSS and the proposed alternatives. The distinctions made between technical severity and security risk enrich the discussion and offer valuable insights which provoked further reading for me.

Cheers

Blessing

References:

1. FIRST ORG. (N.D.). Common Vulnerability Scoring System version 3.1: Specification Document. Available from: https://www.first.org/cvss/specification-document [Accessed 12 October 2023].

2. Spring, J., Hatleback, E. Householder, A. Manion, A. & Shick D. (2021-3). Time to Change the CVSS?. Available from: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=9382369 [Accessed October 9 2023].