Collaborative Learning Discussion 2

Discussion Topic:

Read Spring et al (2021) and then answer the following questions:

What characteristics of CVSS do the authors criticise? Do you agree with the critique? Justify your answer with academic references.

The authors also discuss a number of alternatives to CVSS. Select one of these alternatives and post an argument for why it should replace CVSS.

Initial Post
by Njideka Ozoemena - Thursday, 28 September 2023, 2:36 AM

The article on ''Time to Change the CVSS'' by Spring. et al. (2021) discussed the features, challenges, and mitigation of using Common Vulnerability Scoring System (CVSS) framework in risk assessment of a security system. The article explained that CVSS Risk assessment modelling is designed to identify the technical severity of a vulnerability that helps to assess and prioritise vulnerability management processes where vulnerabilities of different applications are compared. The CVSS generates a score from 0 to 10 based on the severity of the vulnerability and the values are grouped into ranking like Critical, High, Medium, and Low (Risto. J,2023).

The article argues that the CVSS formula is unjustifiable with unreliable outputs as there is no transparency about its formula derivation technique. It buttressed that the major challenge is on calculation of CVSS Scores which are based on qualitative answers and assumptions on effect of a vulnerabilities on Confidentiality, Integrity, and Availability of a system. The articles classified the CVSS challenges under three categories:

Failure to account for context: This is where different organisations have different interpretations of the CVSS scores without addressing the vulnerability context. CVSS does not handle 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.

Failure to account for consequence of vulnerabilities: This is where the severity scoring did not address the material consequence of exploitation of a security attack other than vulnerabilities.

Operational scoring problems: This is challenge of assigning scores based on various inconsistency and assumptions that exploits are common.

I agreed with the identified challenges as the CVSS scoring formula is not transparent on how it is been calculated and the base score grouping element is not realistic because different vulnerabilities is based on different context of an event. Also, according to FORTINET, CVSS scores represent severity of a vulnerability not the security risk that severity brings to specific system.

The article mentioned CVSS-Special Interest Group (SIG) and Quantitative Risk Analysis (QRA) frameworks as an alternative to bridge CVSS gaps. QRA applies to real world problem, it classifies risk according to likehood and impact on a system and this makes it easier to determine which risk an organization should prioritize. QRA offers consistency, allows exploration of range of options for addressing risk, reflect degree of complexity and provides means of analysing the combined effect of risks rather than treating each risk separately (Hillson.D,2020).Risk experts and consultants(Hubbard,2020 Lecture-cast) argues 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).

In conclusion, combination of more than one risk assessment framework on system provides a better result which promotes more reliable risk assessment mitigation policy of a system.

Reference:

Hillson, D. (Thursday December 03,2020) Muti BRIEFS: EXCLUSIVE. Quantitative risk analysis: Strengths and weaknesses Available from: **https://exclusive.multibriefs.com/content/quantitative-risk-analysis-strengths-and-weaknesses/business-management-services-risk-management**[Accessed 27 September 2023].

FORTInet What Is Common Vulnerability Scoring System (CVSS)? Available from: **https://www.fortinet.com/it/resources/cyberglossary/common-vulnerability-scoring-system#:**[Accessed 27 September 2023].

Risto,J.(May 22,2023) SANS What is Common Vulnerability Scoring System (CVSS).Available from :**https://www.sans.org/blog/what-is-cvss/** [Accessed 27 September 2023].

Spring.J, et al. (2021) Time to Change the CVSS? IEEE Securing Privacy Volume:19 issue 2, Available from: **https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/9382369** [Accessed 25 September 2023].

University of Essex Lecturecast(Unit 7),Quantitative Risk Modelling. Available from: **https://www.my-course.co.uk/mod/scorm/player.php?a=11785&currentorg=articulate_rise&scoid=23628&sesskey=SXs9RGFpek&display=popup&mode=normal** [Accessed 22 September 2023].