Learning activity

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

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

2. 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.

Common Vulnerability Scoring System (CVSS)

Introduction: According to the article, Jonathan M. Spring, Eric Hatleback, Allen D. Householder, Art Manion, and Deana Shick | Software Engineering Institute, the authors criticize several characteristics of the Common Vulnerability Scoring System (CVSS). They highlight the lack of transparency and justification in the CVSS formula, inconsistencies in the specification document, and the ranking process of vulnerabilities. The article argues that CVSS fails to consider contextual factors, material consequences, and operational scoring problems. It also suggests that CVSS is used as a risk score without considering the overall risk or the speed of response needed. The authors call for a revision of the CVSS formula to address these limitations and improve vulnerability management.

Furthermore failure to account for context(both technical and human– organizational)and failure to account for material consequences of the vulnerability(whether life or property is threatened) operational scoring problems (inconsistent or clumped scores and algorithm design quibbles).

The article invites readers and prospective authors to share their views on alternative risk scores, the development of a better version

by the CVSS-Special Interest Group (SIG), and how vendors can assess the risk context of their products for diverse customers.

The article also explores the practicality of both quantitative and qualitative modeling in vulnerability assessment The CVSS formula does not consider contextual factors, such as vulnerabilities in shared libraries or the relationship between vulnerabilities.

1. Lack of transparency and justification: The ranking process of vulnerabilities in the CVSS formula is not documented, leading to a lack of transparency and justification.

2. Inconsistency in scoring: Assigning scores to vulnerabilities using CVSS can be inconsistent, as there are vague guidelines and technical details involved.

3. Mis-scoring by security professionals: Security professionals often mis-score vulnerabilities, which can lead to inaccuracies in vulnerability management.

4. Operational scoring problems: The CVSS formula may not adequately address operational scoring problems in vulnerability assessment, such as material consequences of vulnerabilities.

Overall, these limitations and challenges highlight the need for a revision of the CVSS formula to improve vulnerability management.

The authors of “A Way Forward” suggest that the CVSS-Special Interest Group (SIG) should address the flaws in CVSS, not their symptoms. They propose that any new algorithm should aim to address the various risk elements of context and material consequences identified in previous sections of the article.

The authors suggest that adequate user studies should be conducted to understand how organizations use CVSS in their risk assessments today. They also recommend that any replacement

should be accompanied by an empirical study of the consistency of human scoring using it.

Finally, they suggest that advice to the public should be reliable and actionable, and that different contexts should be able to interpret values differently, accounting for each community’s needs, context, and risks. The outputs of the scoring algorithm should be in the form of action categories and never integers. The algorithm itself should be a transparent decision process, not arithmetic. Existing risk assessment methods can be applied for estimating information about expected loss and incorporate this into the decisions as well One alternative to CVSS is the Exploit Prediction Scoring System(EPSS) [3].

EPSS is a data-driven model that aims to estimate the likelihood of a vulnerability being exploited. Unlike CVSS, which focuses on the severity of a vulnerability, EPSS takes into account the potential impact of an exploit. This can provide organizations with valuable insights into the risks they face and help them prioritize their vulnerability management efforts more effectively.

EPSS offers a number of advantages over CVSS.

Firstly, it provides a more dynamic and contextual assessment of vulnerabilities by considering factors such as exploitability, affected assets, and potential attackers. This allows organizations to make more informed decisions about which vulnerabilities to prioritize for patching or mitigation.

Secondly, EPSS leverages machine learning and data analysis techniques to predict the likelihood of exploitation. By analyzing historical exploit data and threat intelligence, EPSS can provide organizations with early warnings and actionable insights to proactively address vulnerabilities before they are actively exploited.

Lastly, EPSS offers a more transparent and justified scoring process compared to CVSS. The data- driven approach of EPSS reduces the subjectivity and inconsistency often associated with manual vulnerability scoring. This transparency allows organizations to have a better understanding of the rationale behind the vulnerability scores and make more informed decisions based on the available data.

Considering these advantages, EPSS presents a promising alternative to CVSS for vulnerability management. Its focus on exploit likelihood and contextual analysis can enhance organizations' ability to prioritize resources effectively and proactively mitigate potential risks.