Collaborative Discussion 2

Peer Review 1

Hello Ayo,

Thank you for such clear writing and analysis of the provided article by Spring et al. (2021). This article raises critical concerns about some characteristics of the Common Vulnerability Scoring System (CVSS) and suggests improvements in vulnerability management. Your review effectively summarises the key criticisms and offers insights into the shortcomings of CVSS discussed by the author.

One key takeaway from this article is when the authors mentioned that CVSS was designed for how vulnerabilities affect traditional IT systems, with equal weighting to confidentiality, integrity, and availability. However, in some cases, data loss is more critical than the loss of control of the device…(Spring et al. (2021)). Every organisation must consider this when addressing risks and vulnerabilities as it is not a one-size-fits-all.

As you rightly mentioned, Exploit Prediction Scoring System (EPSS) as a suggested alternative offers a data-driven and dynamic approach to vulnerability assessment. EPSS considers exploitability, affected assets, and potential attackers, providing a more contextual assessment of vulnerabilities. Integration of machine learning and data analysis techniques enhances the predictive capabilities of EPSS, enabling organisations to address vulnerabilities proactively. This has a notable advantage over

CVSS due to its proactive approach to addressing vulnerabilities. According to an article by HERNÁNDEZ, M. (2022), EPSS looks at the probability of a vulnerability getting exploited. The higher the score, the greater the likelihood that a vulnerability will be exploited. It is worth noting that EPSS is also controlled by the creators of CVSS in conjunction with MITRE creators. The proposed alternative, EPSS, appears promising in addressing the identified shortcomings of CVSS. However, this has faced less scrutiny from experts, perhaps there are hidden flaws that may arise in the future. Overall, I enjoyed reading your post thoughts stirring post.

Cheers

Blessing

References

1. Hernandez, M. (2022). Are vulnerability scores misleading you? Understanding CVSS score. Available from: https://sysdig.com/blog/vulnerability-score-cvss-meaning/. [Accessed October 12 2023].

2. OWASP (2023). API8:2023 Security Misconfiguration. Available from: https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/ Accessed October 13 2023].

3. 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].

Peer Review 2

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].