Discussion 2 – Initial Post

Spring, et al., (2021) have the following criticisms of CVSS scores:

1. The formula for the calculation of CVSS scores '…is not properly justified'.
2. That there is an assumption that there is a linear relationship between CVSS scores and risk.
3. That the statistical techniques used to derive numerical values from ordinal data are questionable.
4. That the CVS equation is derived from data collected from rankings of vulnerabilities by experts, but there is no information about how this process was conducted.
5. The system does not account for organisational context.
6. The system does not account for the effects of vulnerabilities being chained together.

Initially, I am going to attempt to make sense of the mathematics behind the system. I do this purely because it intrigues me, not because I have a particular talent for mathematics. In fact, I have no maths qualification above O Level; but I am going to give it a go anyway!

Analysis of the equations used to produce CVSS values by Chester, (2021) has suggested that they are a 'mathematical sleight of hand' since they contain constants (magic numbers) which have been 'tweaked' to produce a normal distribution of scores between 0 and 10. He concludes:

> "The outcome looks [a] normal [distribution] because it was made to look normal, not because of an underlying process of sampling leading to normality."

Furthermore, Chester, (2021) shows that analysis of actual CVSS report data from 2019, 2020 & 2021 is not normally distributed, the data for each year looks remarkably similar and it is clustered around a few values. Whilst there are other possibilities, he suggests that there is something within the equations themselves that produces these annual similarities and clustering and whilst he is unable to conclusively prove what this is, he makes several interesting observations.

It seems therefore that in not providing a full methodology for the derivation of the equations used to produce CVSS values, FIRST, (2019) have left themselves open to justified criticism, with which I agree. What is interesting is that in recent paper by Sharma, et al., (2022), the authors describe CVSS as a 'quantitative technique'; this is incorrect since CVSS scores are derived from ordinal data and should be seen as rankings only. This clearly demonstrates that misunderstandings regarding the technique are still present.

As far as alternatives to the CVSS system, my research has identified the Exploit Prediction Scoring System (EPSS) first proposed by Jacobs, et al., (2020) and currently at version v2022.01.01. This is a machine learning model which takes numerous data sets about exploitation of a vulnerability 'in the wild' and gives a probability that the vulnerability will be exploited within the next 30 days. This model gives us a measure of 'threat' as opposes to 'risk' for CVSS and could be more easily leveraged to produce mitigation priorities. Analysis provided by the authors, demonstrate the effectiveness of the system but whilst there is a great deal of information provided about the model, the underpinning code and data for the model is not available for critique at the request of 'commercial partners'. Whilst I don't want to come across as cynical, but I would be less suspicious if this were a truly open source project but I feel that it still has its merits.

References

Chester, J. (2021) A Closer Look at CVSS Scores. Available from: https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/ [Accessed 25th April 2023].

FIRST. (2019) Common Vulnerability Scoring System version 3.1: Specification Document. Available from: https://www.first.org/cvss/specification-document [Accessed 25th April 2023].

Sharma, A., Sabharwal, S. & Nagpal, S. (2022) Performance Analysis of Quantitative Software Vulnerability Prioritization Techniques. In: Advances in Intelligent Decision Technologies. Advances in Intelligent Decision Technologies, pp.161–171.

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS?. *IEEE Security & Privacy*, 19 (2), pp.74–78.

Peer Response

by John Bodden - Monday, 1 May 2023, 5:55 PM

Steve, thank you most kindly for your analysis of the CVSS system and the criticism levied against it. It is important to recognise the limitations of any system, especially one that is used widely in cybersecurity.

The criticism regarding the assumption of a linear relationship between CVSS scores and risk and the questionable statistical techniques used to derive numerical values from ordinal data are valid points. It is important to consider the limitations of any system that attempts to quantify risk (DNV, n.d.).

The lack of information about the process used to collect the data for the CVS equation is also a concern, as this could impact the validity of the results. Additionally, the fact that the system does not account for organisational context or the effects of vulnerabilities being chained together further limits its usefulness.

The Exploit Prediction Scoring System (EPSS) you mentioned as an alternative to the CVSS system is an interesting option. However, the fact that the underpinning code and data for the model are not available for critique is a concern, as transparency and openness are important in cybersecurity.

Overall, it is important to recognise the limitations of any system used to quantify risk and to consider multiple approaches when making decisions about cybersecurity.

References

DNV, n.d. *Why quantify risks? Good and bad reasons for quantifying risks.* [Online] Available at: https://www.dnv.com/article/why-quantify-risks-good-and-bad-reasons-for-quantifying-risks-200533
[Accessed 29 April 2023].

Discussion 2: Summary Post

My initial post focussed on the work of Spring et al., (2021) and their criticisms of the Common Vulnerability Scoring System (CVSS) and in particular, the calculations underpinning the system.

These criticisms aside, since CVSS is currently the recommended system for compliance by major oversight bodies such as the National Institute of Standards in Technology (NIST) and the Payment Card Industry Data Misuse Security Standard (PCI DSS) (Spring et al., 2021), its efficacy requires further investigation.

One of the main issues, as far as I can tell, has centred around the distinction between severity and risk; this issue seems to have been of the authors own making since in earlier versions of CVSS it was clear that the intent was to provide a measure of risk (Mell et al., 2007). This seems to be what prompted its recommendation by NIST and PCI DSS. Concerns were raised by security professionals regarding this issue e.g., Robinson, (2019). The paper by Spring, (2021) [the 2021 paper is an updated version of the paper originally published in 2018 “Towards improving CVSS.”] prompted a revision and the release of Version 3 of the CVSS where the authors set out to change the narrative by clearly stating that CVSS should be used as a measure of risk, not severity (First, 2019). Unfortunately, there is still ambiguity in the documentation regarding this issue as highlighted by Howland, (2022) who goes on to further investigates the efficacy of CVSS version 3 and is forthright in his conclusion:

> *“CVSS is laden with issues. There is no clear reasoning given as to how the system was devised, it is riddled with logical inconsistencies, and it is only able to partially account for the context of a vulnerability, as well as being an empirically poor means of representing a vulnerability’s severity.[…] the CVSS-SIG must make radical changes to the standard in the imminent CVSS v4 backed up by transparent efficacy testing, or a new remediation prioritization system should be adopted.”*

It would seem clear that CVSS is not fit for purpose and a new approach is required to enable practitioners to easily calculate contextual risk and hence prioritise mitigations.

References

FIRST. (2019) Common Vulnerability Scoring System version 3.1: Specification Document. Available from: https://www.first.org/cvss/specification-document [Accessed 10th May 2023].

Howland, H. (2023) CVSS: Ubiquitous and Broken. *Digital Threats: Research and Practice*, 4 (1): 1–12. doi:10.1145/3491263.

Mell, P., Scarfone, K & Romanosky, S. (2007). The common vulnerability scoring system (CVSS) and its applicability to federal agency systems. Available from: https://www.govinfo.gov/content/pkg/GOVPUB-C13-19c8184048f013016412405161920394/pdf/GOVPUB-C13-19c8184048f013016412405161920394.pdf [Accessed 10th May 2023].

Robinson, C. (2019). Why CVSS does not equal risk: How to think about risk in your environment. Available from: https://www.redhat.com/en/blog/why-cvss-does-not-equal-risk-how-think-about-risk-your-environment [Accessed 10th May 2023].

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS? *IEEE Security & Privacy*, 19 (2), pp.74–78.