Initial Post

In the article named "Time to Change the CVSS?" the authors Spring et al. object several aspects of the Common Vulnearbility Scoring System (CVSS). They criticise the following:

- Calculation method lacks empirical or theoretical support.
- CVSS converts qualitative answers to a numerical scale.
- The intransparent process of the CVSS formula.
- Undocumented initial ranking of vulnerabilities by experts.
- Lack of transparency regarding the weighting of metrics.

I agree with the critical arguments of the authors, but on the other hand I am of the same opinion as Hughes and Robinson (2024) who mention, that “It is worth noting that prior to CVSS the industry used incompatible and custom rating systems to try to communicate vulnerability severities. Despite many valid critiques of CVSS and how it is often used, it is inarguably the most formalized and widely adopted system for vulnerability scoring in the industry as of this writing.”

In addition, CVSS is continuously being updated with the current version CVSS v4.0, released in November 2023 (Kimberll, 2023).

The authors propose a new system called Stakeholder-Specific Vulnerability Categorisation (SSVC), which focuses on decision-making rather than numerical scores, unlike CVSS. SSVC uses qualitative methods, such as decision trees or priority categories, to guide stakeholders based on specific contexts, impacts, and organisational needs, allowing for a more relevant and actionable response tailored to each organisation's unique circumstances (Householder et al., 2021).

Word count: 227

References:

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS?. *IEEE Security & Privacy* 19(2): 74-78. DOI: https://doi.org/10.1109/MSEC.2020.3044475

Hughes, C. & Robinson, N. (2024) Vulnerability Scoring and Software Identification. *Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem* 1: 79-114 DOI: https://doi.org/10.1002/9781394277155.ch5

Kimberll, A. (2023) FIRST Announces CVSS v4.0 release. Available from: https://www.redhat.com/en/blog/first-announces-cvss-v40-release [Accessed 9 September 2024]

Householder, F., Hatleback, E., & Spring, J. (2021). A Stakeholder-Specific Vulnerability Categorization. *SEI Podcast Series*. [Podcast]. Available from: https://apps.dtic.mil/sti/citations/AD1146956 [Accessed 9 September 2024]

Peer Response 1

Hi Gesine,
Thank you for the valuable points made in your post.

The critique of the Common Vulnerability Scoring System (CVSS) presented by Spring et al. (2021), which you have agreed on, is valid and well supported by existing literature. Eventhough CVSS is widely used, it often struggles to capture the full complexity of evolving threats. Its results can be oversimplified and does not take different views into account. A specific risk can be given different weightings by different departments in an organisation.

As you have hightlited in your post, it can be difficult to deal with the rapidly changing threat environment. This has also been mentioned by Howland (2023) “As of Q2 2021, CVSS’s scoring system is only on its second version in its 14-year history as the first version was scrapped immediately after creation with CVSS v2 released in June 2007, effectively acting as the first deployed version.”

The Cyber-Physical Resilience Metric (CPRM) focuses on Cyber-Physical Systems (CPS) which integrate computational components with physical processes. These systems combine sensing, computation, control, and networking to interact with the physical world in real-time, often in safety-critical environments (Segovia et al., 2020). Hence this could not be a valid alternative to CVSS, since it only covers a fraction of threats compared to CVSS.

Word count: 212

References:
Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS?. *IEEE Security & Privacy* 19(2): 74-78. DOI: https://doi.org/10.1109/MSEC.2020.3044475

Howland, H. (2021) CVSS: Ubiquitous and Broken. *Digital Threats: Research and Practice* 4(1): 1-12. DOI: https://doi.org/10.1145/3491263

Segovia, M., Rubio-Hernan, J., Cavalli, A., & García-Alfaro, J. (2020) Cyber-Resilience Evaluation of Cyber-Physical Systems. *IEEE 19th International Symposium on Network Computing and Applications (NCA)* DOI: https://doi.org/10.1109/nca51143.2020.9306741

Peer Response 2

Hi Irina,
Thank you for sharing your thoughts about CVSS.

While the latest version of CVSS was recently published and offers significant improvements over its predecessor, the system still fails to address important aspects such as inadequate representation of real-world risk and Limited scope and lack of context, which includes the potential for chained exploits (Divinsky, 2023).

I would argue that the chaining of different vulnearbilities is an easy to understand topic and neither is the modelling of such threats. Robinson (2022) concluded in her paper named “An Exploratory Study into Vulnerability Chaining Blindness Terminology and Viability” that IT and cybersecurity professionals often lack awareness of vulnerability chaining, a term that refers to the potential compounding effects of multiple vulnerabilities. Although cybersecurity professionals acknowledge its importance, the term is not well-understood or used widely across the board, especially within IT operations teams. There is a gap bewtween IT and cybersecurity professionals. While both groups recognise the need for holistic, risk-based management of security, IT professionals are more concerned with system functionality and user needs, rather than focusing on the broader implications of lower-priority vulnerabilities that could be exploited in combination. On the other hand, cybersecurity professionals see the value in addressing these vulnerabilities but struggle with the complexity and sheer volume of information required to implement defense in depth effectively.

Word count: 220

References:
Divinsky, Y. (2023) CVSS v4.0 - what you need to know. Available from: https://vulcan.io/blog/cvss-v4-0-what-you-need-to-know/ [Accessed 22 September 2024]

Robinson, N. (2022) An Exploratory Study into Vulnerability Chaining Blindness Terminology and Viability. *ArXiv.org*. DOI: https://doi.org/10.48550/arXiv.2203.10403

Summary Post

Hi Gesine, Hi David,

Thank you both for your valuable responses and contribution on this discussion.

As we all agree on the critique made by Sprint et al. (2021) and have found the Stakeholder-Specific Vulnerability Categorization (SSVC) framework as an alternative, the question arises whether SSVC is the holy grail or just another framework which contains flaws, such as CVSS.

SSVC was introduced in April 2021 by security researchers at Carnegie Mellon University's Software Engineering Institute (SEI) and the Cybersecurity and Infrastructure Security Agency (CISA). It was created to help security analysts and vulnerability managers with vulnerability prioritisation decision-making and is based on the decision tree model. SSVC relies on manual input of values from an organisation, which implies the method is not scaleable and every organisation has to figure out how severe a certain vulnerability is to them (Keizman, 2024). This is one of the two limitations which even the authors of the SSVC white paper acknowledge, the other being the additional data which is needed and might not be available in every organisation (Spring et al., 2021).

In summary, it can be said that SSVC can function as an addition to CVSS. As my fellow student David rightly concluded, a hybrid approach makes most sense.

Word count: 207

References:

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS?. *IEEE Security & Privacy* 19(2): 74-78. DOI: https://doi.org/10.1109/MSEC.2020.3044475

Keizman, O. (2024) The SSVC risk prioritization method: what it is, when to use it, and alternatives. Available from: https://vulcan.io/blog/the-ssvc-risk-prioritization-method-what-it-is-when-to-use-it-and-alternatives [Accessed 23 September 2024]

Spring, J., Householder, A., Hatleback, E., Manion, A., Oliver, M., Sarvapalli, V., Tyzenhaus, L., & Yarbrough, C. (2021) *Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization (version 2.0)*. Available from: https://insights.sei.cmu.edu/documents/606/2021_019_001_653461.pdf [Accessed 23 September 2024]