Collaborative Discussion 2
Initial Post

CVSS

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. (Mell et al., 2022)

CVSS criticism

Weaknesses in the existing CVSS scoring system have been highlighted through new research, with existing metrics deemed responsible for "overhyping" some vulnerabilities.

So-called "overinflated" ratings are potentially eating up the limited time of cybersecurity teams who may then not be focused on the bugs most likely to impact their organizations in favor of issues deemed critical across the board. (Charlie Osborne,2023)

Alternative of CVSS

Risk-based vulnerability management assesses the exact risk levels, prioritizes the vulnerabilities, and mitigates them to reduce the probability of exploitation. (Priyanka VH, 2022)

CVSS vs DREAD

STRIDE is a Threat modelling framework that is used to Identity threats in the application architecture early when they are less costly to mitigate. As a result, it greatly reduces the total cost of development and improves the security posture of the application. STRIDE stands for:-	**DREAD threat modelling framework is comparable to CVSS, The Common Vulnerability Scoring System (CVSS) is a framework for measuring the severity of vulnerabilities. It is important to note that since CVSS is there to measure vulnerabilities, we cannot measure threats with CVSS because we do threat modelling**

- Spoofing (change state) **- Tampering (Man in the middle, IDOR)** **- Repudiation (denying activities)** **- Information disclosure (data breach)** **- Denial of service (service unavailable)** **- Elevation of privilege (performing actions of a high privileged user)**	**on the design and architecture level.**

(Cerovic L.(2022) StrideLang)

Reference:

Reference:

Charlie Osborne (2023) CVSS system criticized for failure to address real-world impact. Available at: https://portswigger.net/daily-swig/cvss-system-criticized-for-failure-to-address-real-world-impact

Priyanka VH (2022) Why Is It Important To Prioritize Vulnerabilities Beyond CVSS Available at: https://www.secpod.com/blog/why-is-it-important-to-prioritize-vulnerabilities-beyond-cvss/

Cerovic L.(2022) Creation of a Domain-Specific Threat Modeling Language using STRIDE, DREAD and MAL. KTH Royal institute of technology. Available from : https://kth.diva-portal.org/smash/get/diva2:1710734/FULLTEXT01.pdf.

Summary post

It is in my opinion that CVSS (Common Vulnerability Scoring System) is a quantitative measure. The point that assigned to a vulnerability is a numerical value that indicates the relative severity of the vulnerability. The CVSS score is calculated based on various of qualitative and quantitative factors, across from complexity of the attack required to exploit the vulnerability, the potential threat of the vulnerability, and the number of users or systems impact (NIST, 2022). Nonetheless, as it is measured in a numeric value (0-10), it may fall under the category of quantitative measurement. (Oracle 2016) In conclusion , it is suggested that CVSS is a free industry standard for assessing the security of computer system. Score would be assigned for the vulnerability by means to help security administrators to prioritize the problem.

Tracing back to the record, CVSS first appeared in 2005 and has changed over time. The latest version of CVSS is CVSSv3.1, which was firstly

introduced in 2019. The score assigned to a vulnerability reflects the vulnerability's potential impact on the system if it is exploited, as well as the difficulty of exploiting the vulnerability.

The CVSS scoring system ranges from 0 to 10, with a score of 10 indicating the most severe vulnerability. The system takes into account a number of factors, such as the level of access required to exploit the vulnerability, the specific impact that exploitation would have on the system, and the exploitability of the vulnerability. (Claus Neilsen—June 7, 2022)

Despite CVSS has been widely used by many experts , following frameworks serve as alternatives that are also recommended by experts.

1. Common Weakness Enumeration (CWE): Focuses on software weaknesses that can lead to vulnerabilities, rather than the vulnerabilities themselves. (CWE ,2014)

2. The Open Web Application Security Project (OWASP) Risk Rating Methodology: focuses on web application vulnerabilities and provides a risk rating based on the likelihood of a vulnerability being exploited and the potential impact of an attack.(Grant Onger ,2023)

3. National Institute of Standards and Technology (NIST) Cybersecurity Framework: Rather than focusing on specific vulnerabilities, NIST Framework offers a comprehensive approach to managing cybersecurity risk. The framework provides guidance on identifying, assessing, and managing risk across an entire organization.

Reference

CWE 2014 aviable at https://cwe.mitre.org/cwss/cwss_v1.0.1.html

Grang Onger 2023 aviable at https://owasp.org/blog/2023/03/31/owasp-strategy-2023-1.html

Claus Nielsen—June 7, 2022 avaiable at https://www.holmsecurity.com/blog/cvss-and-why-it-is-necessary

Maximum rating: (1)
PermalinkReply

Peer Response to Stella William
Thank you for bringing up the critism of CVSS, as there are indeed some potential issues existed in this framwork that users have to beware of.

First, CVSS relies on subjective assessments by security experts, and different experts may assign different scores to the same vulnerability. This can lead to inconsistencies in ratings and can make it difficult for organizations to prioritize which vulnerabilities to address first. (2020)

Second, CVSS scores do not take into account factors such as the potential impact on business operations, the specific context of an organization's environment, or the likelihood of a successful attack. This can result in an overemphasis on the technical characteristics of a vulnerability, rather than its actual risk to the organization. (Spring J 2021)

Finally, CVSS ratings are based solely on the characteristics of the vulnerability itself, rather than the effectiveness of existing mitigations or the overall security posture of an organization. As a result, CVSS scores may not fully reflect the true risk posed by a vulnerability to a particular organization.

References
·Aboud, J. (2020) Why You Need to Stop Using CVSS for Vulnerability Prioritization. 27 April 2020. Tenable Research. Available from: https://www.tenable.com/blog/why-you-need-to-stop-using-cvss-for-vulnerability-prioritization [Accessed 23 Apr. 2023]
·Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D. (2021) Time to Change the CVSS. IEEE Security & Privacy 19(2): 74–78. DOI: https://doi.org/10.1109/msec.2020.3044475
Maximum rating: -

It is in my opinion that CVSS (Common Vulnerability Scoring System) is a quantitative measure. The point that is assigned to a vulnerability is a numerical value that indicates the relative severity of the vulnerability. The CVSS score is calculated based on various of qualitative and quantitative factors, across from complexity of the attack required to exploit the vulnerability, the potential threat of the vulnerability, and the number of users or systems impact (NIST, 2022). Nonetheless,as it is measured in a numeric value (0-10), it may fall under the category of quantitative measurement. (Oracle 2016)

References

NIST 2022 aviable at https://nvd.nist.gov/vuln-metrics/cvss
Oracle 2021 aviavle at https://docs.oracle.com/cd/E74890_01/books/SecurHarden/securharden_testing002.htm

Maximum rating: -