Initial Post

by Kwok Wai Yau - Friday, 30 September 2022, 3:46 PM
Number of replies: 2

The CVSS formula, which is used to calculate CVSS scores, is one of the main problems. The CVSS formula, which is used to calculate CVSS scores, is one of the main problems. The equations appear to be the product of procedures that may or may not be accurate, but the CVSS literature is opaque on how its formulas were derived. The relationship(s) between vulnerabilities are not handled by CVSS. Independent scoring may be inaccurate for several reasons, one of which being the possibility of chaining vulnerabilities together and using one to provide the prerequisites for another (Spring et al 2, 2021).

Furthermore, the author also stated that flaws other than vulnerabilities can also result in security incidents in information systems. With equal weights given to confidentiality, integrity, and availability, CVSS was created to account for how vulnerabilities affect conventional IT systems. However, in other circumstances, such as when it comes to financial systems or personal user data, data loss might be more serious than losing control of the device. Other situations, such as safety-critical embedded devices used in healthcare and industrial control systems, place a greater emphasis on data availability or integrity (Spring et al 2, 2021).

I do agree with the authors. No matter how probable they are to be exploited, 56% of all vulnerabilities are rated as High (CVSS score of 7.0-8.9) or Critical (CVSS score of 9.0-10.0), according to Tenable Research. Additionally, security teams utilising CVSS to prioritise their efforts are wasting the bulk of their time on the incorrect issues because more than 75% of all vulnerabilities with a score of 7 or higher have never had an exploit released against them. (Spring et al 2, 2021)

Organizations should base their security decisions on risk, but CVSS does not offer the full picture—even after taking into consideration the temporal and environmental ratings meant to take context and effects into account. The modeling does not provide any insight into the uncertaintyof the risk analysis but rath er provides an excellent ranking of source variables. (Emblemsvåg, Jan & Kjølstad, Lars., 2006)

The authors discuss a number of alternatives to CVSS like few Stakeholder-Specific Vulnerability Categorization (SSVC). It is a system for ranking the importance of various vulnerability management actions. Since there are so many distinct parties involved in vulnerability management, SSVC try to stay as far away from one-size-fits-all solutions as they can. For many communities involved in vulnerability management, it takes the shape of decision trees. The outcome of using SSVC is a priority choice. (Muhammad Akbar, 2020)(Allen Householder, 2019).

Reference:

Spring, J., Hatleback, E., Householder, A., Manion, A., Shick, D., (2021). Time to Change the CVSS? Available at: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/9382369 [Accessed 29 September 2022].

Aboud, J. (2020) Why You Need to Stop Using CVSS for Vulnerability Prioritization. Available at: https://www.tenable.com/blog/why-you-need-to-stop-using-cvss-for-vulnerability-prioritization [Accessed 29 September 2022].

Emblemsvåg, Jan & Kjølstad, Lars. (2006). Qualitative risk analysis: Some problems and remedies. Management Decision - MANAGE DECISION. 44. 395-408. 10.1108/00251740610656278.

Akbar, M. (2020) A Critical First Look at Stakeholder Specific Vulnerability Categorization (SSVC). Available at: https://blog.secursive.com/posts/critical-look-stakeholder-specific-vulnerability-categorization-ssvc/ [Accessed 29 September 2022].

Householder, A. (2019). Prioritizing Vulnerability Response with a Stakeholder-Specific Vulnerability Categorization. https://insights.sei.cmu.edu/blog/prioritizing-vulnerability-response-with-a-stakeholder-specific-vulnerability-categorization/ [Accessed 29 September 2022].