Collaborative Learning Discussion 2 -> Initial Post

by Gokul Kurunthasalam - Thursday, 20 October 2022, 4:26 PM

What characteristics of CVSS do the authors criticise? Do you agree with the critique? Justify your answer with academic references.

CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them or how quickly they should respond to a vulnerability. If so, then either CVSS needs to change, or the community needs a new system.

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 safety-critical embedded devices used in healthcare and industrial control systems, place a greater emphasis on data availability or integrity. It is possible to change the relative weights of secrecy, integrity, and availability using the CVSSv3.1 Environmental metrics. It is unclear whether the Environmental metrics offer a solid and sufficient remedy, though, as this change is mediated by the CVSS formula, which is opaque and unjustified. Additionally, additional design tenets for conventional IT flaws may be incompatible with flaws in other fields. (J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, March-April 2021)

The authors also discuss a number of alternatives to CVSS. Select one of these alternatives and post an argument for why it should replace CVSS.

Stakeholder-Specific Vulnerability Categorization (SSVC)

SSVC uses a decision-tree method that can be used by vulnerability management teams as well as developers. instead of putting a dollar value on vulnerabilities, it uses a cost-benefit analysis. {Kitty Kioskli, Nineta Polemi, 2022)

Vulnerability prioritization (VPR)

Combines the risk of exploitation with the technical CVSS rating. examines a number of different types of intelligence to get a score that is more comprehensive. decreases the quantity of High and Critical vulnerabilities to ease the burden of patching. (Muhammed Fatih Bulut, Abdulhamid Adebayo, Daby Sow, Steve Ocepek, 2022)

References:

J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, "Time to Change the CVSS?," in IEEE Security & Privacy, vol. 19, no. 2, pp. 74-78, March-April 2021, doi: 10.1109/MSEC.2020.3044475.

Kitty Kioskli, Nineta Polemi "Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores." Human Factors in Cybersecurity, Vol. 53, 2022, 138–150; https://doi.org/10.54941/ahfe1002211

Muhammed Fatih Bulut, Abdulhamid Adebayo, Daby Sow, Steve Ocepek, "Vulnerability Prioritization: An Offensive Security Approach" Submitted on 22 Jun 2022; Cornell University; https://doi.org/10.48550/arXiv.2206.11182