

Collaborative Learning Discussion 2

In reply to Kwok Wai Yau

Peer Response - 1

by [Gokul Kurunthasalam](#) - Friday, 21 October 2022, 3:42 PM

I appreciate your post and I would take this as an opportunity to add a few more points. The CVSS formula, which is used to calculate CVSS scores, is one of the main problems. You must respond to eight questions about the attack vector, the privileges required for an attacker to take advantage of the vulnerability, the impact on the confidentiality, integrity, and availability of the system, and other topics to arrive at a CVSS v3.0 base score.

Employing inconsistent output, CVSS is used by enterprises to "properly analyse and prioritise their vulnerability management activities." We contend that both for its intended use and as a stand-in for risk to a susceptible system, the present CVSS version continues to be insufficient. This essay will list the reasons why the CVSS formula is flawed and how it fails to adequately educate vulnerability management before offering a solution to these issues. (J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, March-April 2021)

There are a number of ways whereby CVSS fails to take context into account generally. These include shared library vulnerabilities, connected or chained vulnerabilities, general web vulnerabilities, and various communities' interpretations of a CVSS score.

Prioritizing actions during vulnerability management is done using the Stakeholder-specific Vulnerability Categorization (SSVC) system. By focusing on a modular decision-making framework with clearly defined and tried-and-true components that vulnerability managers can choose and employ as suitable to their context, SSVC seeks to avoid one-size-fits-all solutions. (Jonathan Spring, Eric Hatleback, Allen D. Householder, Art Manion, Deana Shick, 2019)

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.

Jonathan Spring, Eric Hatleback, Allen D. Householder, Art Manion, Deana Shick "Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization" Carnegie Mellon University; DECEMBER 2019; <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379>