**CVSS**

The authors have opined that the usage of Common Vulnerability Scoring System (CVSS) as a risk score is a mistake, and have particularly criticised the CVSS scoring algorithm/formula as they claim it needs empirical justification. They argue that weighing confidentiality, integrity and availability equally among individuals and organisations is misleading (Spring et al., 2021. They further argue that CVSS scores severity as against security risks, CVSS scoring is opaque (does not account for specifics, and items in context).

**Recommendation**

The Stakeholder-Specific Vulnerability Categorization (SSVC) is an attempt to fix the issues the authors have highlighted. This is in addition to an alternative proposed whereby adequate user studies be carried out to understand how organisations use CVSS in their risk assessments. I agree with the authors on the new recommendation, as it provides a more transparent yardstick of measuring vulnerability management and cybersecurity concerns – grounded in careful reasoning, which incorporates transparency and empirical evidence (Spring et al., 2021).

**Conclusion**

The CVSS seems to be widely accepted scoring system; however, industry experts are beginning to raise questions on its transparency - which further adds a dent on its integrity. A new scoring system needs adoption that incorporates the good of the CVSS in addition to the fixes from the CVSS’s flaws.

**Reference**

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) 'Time to Change the CVSS?', IEEE Security & Privacy, 19(3), pp. 70-75. Available at: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/9382369 (Accessed: 10 November 2024).