Collaborative Discussion 2 – CVSS - Initial Post

1. Discussion

1.1. Spring et al.'s Common Vulnerability Scoring System (CVSS) Critique

Spring et al. (2021) criticise CVSS version 3.0 as being inadequate for both its intended use - rating the severity of a vulnerability and to assist companies in prioritising their response (FIRST, 2015) and for its common use - as a method to assess risk (Spring et al., 2021).

Spring et al. (2021) point out 3 specific errors of the system that they believe need addressing:

- Failure to account for context.
- Failure to account for material consequences of the vulnerability (whether life or property is threatened).
- Scoring inconsistencies.

Their conclusion is that the CVSS must change or that it should be replaced by a more effective system.

1.2. Analysis

The criticisms are valid. FIRST considered exposure and threat outside the scope of CVSS v3.x (FIRST, 2019), which limited the ability to take a complete view of a vulnerability. Wunder et al. (2024) confirmed inconsistent scoring and linked it to the nature of the system. They found approximately 30% of users do not consult the CVSS user guide.

Consequently, FIRST released CVSS version 4, which addresses these issues (FIRST, 2023):

- Base metrics can be modified to fit an organisation's environment.
- Supplemental metrics are introduced adding more contextual information to a vulnerability.
- Scoring system adjustment for less variation.

There are still issues with v4.0: Environmental scores require users to be familiar with CVSS metrics to be implemented - many users are not (Aggarwal, 2023). Balsam et al. (2024) concluded that the spread of scores was unnatural in some ranges.

These issues show the fixes were incomplete. Complaints were addressed and improved the system technically, but not in a way that fundamentally improved the functionality for practical use.

2. Recommendations

The suggestion that CVSS can be replaced by another system is unrealistic, due to CVSS being embedded into cyber security culture at several high-profile institutions. The National Institute of Science and Technology (NIST) promotes its use and has a CVSS calculator on its website (NIST, 2025). The Payment Card Industry Data Security Standard (PCI DSS) historically required vulnerability checks using CVSS for compliance (PCI, 2015).

A practical solution would be combining CVSS v.4 with another system that would be more functional and likely to be widely adopted.

One suitable partner is Exploit Prediction Scoring System (EPSS) which measures the likelihood of vulnerabilities being exploited practically (FIRST, 2025). Tan et al. (2025) found that the two systems had no correlation, showing they evaluate different areas and allowing them to complement each other. Howland (2022) says that EPSS has limitations for generating risk scores and supports the idea of it being used in combination with other systems.

3. References

Aggarwal, M. (2023) 'A Study of CVSS v4.0: A CVE Scoring System', *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Gautam Buddha Nagar, India. Pp. 1180-1186. Available at: https://doi.org/10.1109/IC3I59117.2023.10397701

Balsam et al. (2024) 'Comprehensive comparison between versions CVSS v2.0, CVSS v3.x and CVSS v4.0 as vulnerability severity measures', *2024 24th International Conference on Transparent Optical Networks (ICTON)*, Bari, Italy. Pp. 1-4. Available at: https://doi.org/10.1109/ICTON62926.2024.10647452

FIRST. (2015) *Common Vulnerability User Guide v3.0; User Guide.* Available at: https://www.first.org/cvss/v3-0/cvss-v30-user_guide_v1.6.pdf (Accessed 11 September 2025).

FIRST. (2019) *Common Vulnerability User Guide v3.1; User Guide.* Available at: https://www.first.org/cvss/v3-1/user-guide (Accessed 12 September 2025).

FIRST. (2023) *Common Vulnerability Scoring System version 4.0; Specification Document.* Available at: https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf (Accessed 12 September 2025).

FIRST. (2025) *EPSS: Exploit Prediction Scoring System*. Available at: https://www.first.org/epss/ (Accessed 11 September 2025).

Howland, H. (2022) 'CVSS: Ubiquitous and Broken', *Digital Threats: Research and Practice*, 4(1), pp. 1-12. Available at: https://doi.org/10.1145/3491263

NIST. (no date) *National Vulnerability Database: Common Vulnerability Scoring System Calculator*. Available at: https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator (Accessed 12 September 2025).

PCI Security Standards Council. (2015) *PCI DSS Quick Reference Guide*. Available at: https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (Accessed 11 September 2025).

Spring et al. (2021) 'Time to Change the CVSS', *IEEE Security & Privacy*, 19(2), pp. 74-78. Available at: https://doi.org/10.1109/MSEC.2020.3044475

Tan et al. (2025) 'Analysis of Vulnerability Severity and Exploit Probability Scoring Frameworks: CVSS and EPSS', *2025 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA. Pp. 54-59. Available at: https://doi.org/10.1109/SIEDS65500.2025.11021216

Wunder et al. (2024) 'Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities,' *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA. Pp. 1102-1121. Available at: https://doi.org/10.1109/SP54263.2024.00058