**Evolving Standards in Cybersecurity Vulnerability Assessment Over Time**

Blake Meyer, Information Technology, College of Engineering and Computer Science

**Research Statement**

This research aims to investigate the evolution of CVE (Common Vulnerabilities and Exposures) vulnerability assessment scoring systems to understand how these changes have impacted cybersecurity practices. It will explore the modifications in the scoring criteria, the rationale behind these changes, and their effectiveness in addressing the constantly changing landscape of cybersecurity threats. By analyzing historical and current CVE scoring methodologies, this study seeks to highlight the advancements made in vulnerability assessment and propose recommendations for future improvements.

**Introduction**

The Common Vulnerabilities and Exposures (CVE) system serves as a crucial benchmark in the cybersecurity landscape, offering a unified identifier for the cataloging of security vulnerabilities and exposures. Initiated to provide clarity and common understanding within the cybersecurity community, the CVE system has become instrumental in facilitating the effective communication of vulnerability attributes across various platforms and tools. The vulnerability assessment scoring that accompanies CVEs, primarily through systems like the Common Vulnerability Scoring System (CVSS), has undergone significant evolution to keep pace with the increasingly sophisticated landscape of cybersecurity threats. This evolution reflects a dynamic effort to enhance the precision and utility of vulnerability assessments, aiming to provide stakeholders with actionable information that accurately reflects the risk posed by identified vulnerabilities.

The adoption of the CVE scoring system was driven by the necessity for a standardized approach to assess and communicate the severity of vulnerabilities. Initially, the system sought to offer a straightforward, universally applicable set of standards that could be used to prioritize response actions based on the severity of vulnerabilities. However, as cyber threats have evolved in complexity and impact, so too has the scoring system, adapting to incorporate a broader range of metrics and more advanced assessments of risk. This research dives into the origins and development of the CVE scoring system, examining the important moments and modifications that have shaped its current form. By analyzing a selection of peer-reviewed journal articles, official cybersecurity frameworks, and expert analysis, the study aims to map out the trajectory of CVE scoring modifications. It will explore the theoretical foundations and practical considerations that have informed these changes, including the integration of user and environmental metrics in the CVSS v3.x enhancements, which offer a more detailed assessment of vulnerabilities. Additionally, this study will evaluate the impact of CVE scoring evolution on cybersecurity management practices and threat mitigation strategies. It will consider how changes in the scoring system have influenced the prioritization of vulnerabilities and the resources allocated for their remediation. By employing theoretical frameworks from cybersecurity standards and risk assessment methodologies, the investigation seeks to highlight the significance of these developments for enhancing cybersecurity resilience. The evolution of CVE scoring is not just a technical adjustment; it represents a critical aspect of the ongoing effort to fortify digital infrastructures against the backdrop of an ever-changing threat landscape. This review will underscore the crucial role of CVE scoring in the broader context of cybersecurity management and its implications for future vulnerability assessment practices.

Research Methodology

The research methodology for this project proposal on the evolution of Common Vulnerabilities and Exposures (CVE) vulnerability assessment scoring will be focused on a comprehensive analysis of both academic journal articles and empirical CVE/CVSS data. This approach allows for a thorough investigation into how CVE scoring systems have adapted over time to address the shifting landscape of cybersecurity threats, and the implications of these changes on vulnerability management practices.

### Journal Article Analysis

The first component of the research methodology involves a review of peer-reviewed journal articles. This review will focus on articles that discuss the development, application, and impact of CVE and CVSS scoring systems. Selection criteria for these articles will include relevance to the research questions, contribution to the field of cybersecurity, and publication date to ensure the timeliness of the data. Using content analysis, the study will extract insights regarding the theoretical foundations of CVE/CVSS scoring, historical milestones in their evolution, and academic debates surrounding their effectiveness and limitations. This qualitative analysis will help identify patterns, themes, and gaps in the existing literature, providing a scholarly context for understanding the changes in CVE scoring systems.

### CVE/CVSS Data Analysis

The second component focuses on the quantitative analysis of actual CVE and CVSS data. This analysis will involve collecting data sets from authoritative sources, such as the National Vulnerability Database (NVD), which maintains a comprehensive database of standardized vulnerability management data. The study will examine changes in the distribution of CVSS scores over time, the frequency and types of vulnerabilities reported, and any notable trends in vulnerability severity. By employing statistical methods, the research will assess how the evolution of scoring criteria has potentially influenced the characteristics of reported vulnerabilities. This empirical analysis aims to provide concrete evidence of the impact of CVE/CVSS scoring system modifications on the cybersecurity community's ability to assess and prioritize vulnerabilities.

### Integration of Findings

Integrating insights from both the journal article analysis and CVE/CVSS data analysis will allow for a multifaceted understanding of the research topic. This integration will enable the study to not only track the historical and theoretical evolution of CVE scoring systems but also to correlate these developments with actual changes in the scoring of vulnerabilities over time. The combined findings will offer a comprehensive picture of the role and effectiveness of CVE/CVSS scoring systems in cybersecurity vulnerability management.

This research methodology, with its emphasis on both qualitative and quantitative analysis, is designed to provide a well-rounded exploration of the evolution of CVE scoring systems. It will contribute to a deeper understanding of the challenges and successes in standardizing vulnerability assessments and the ongoing efforts to adapt these critical tools to meet the demands of an ever-evolving cybersecurity landscape.

**IRB/IACUC Statement:**This project does not require IRB or IACUC approval, as it involves the analysis of publicly available data and professional interviews without collecting sensitive personal information.

**Expected Outcomes**

Upon the completion of this research project on the evolution of Common Vulnerabilities and Exposures (CVE) vulnerability assessment scoring, several key outcomes are anticipated. The primary outcome will be a comprehensive research paper detailing the findings of the study, aimed for submission to a respected scholarly journal in the field of cybersecurity. This paper will encapsulate the historical evolution of CVE scoring, the impact of these changes on vulnerability assessment practices, and insights into the future direction of vulnerability scoring systems. Additionally, a poster presentation will be prepared for publicizing at an undergraduate research conference, offering an overview of the research findings, methodologies employed, and the implications of the study. This format will facilitate direct engagement with peers, faculty, and industry professionals, fostering opportunities for feedback and collaboration.

Additionally, the project will produce a white paper designed to communicate the practical implications of the research findings to a broader audience, including cybersecurity practitioners, policy makers, and community members. The white paper will emphasize actionable recommendations for improving vulnerability assessment processes and will be shared through relevant online platforms and social media to maximize its reach and impact.

The research is expected to contribute new knowledge and understanding to the field of cybersecurity by elucidating how the CVE scoring system has adapted to the evolving threat landscape and by highlighting the practical impacts of these changes on vulnerability management practices. It will offer a critical analysis of the scoring system's effectiveness in accurately reflecting the severity of vulnerabilities and guiding remediation priorities. For the academic community at the University of Central Florida (UCF), this study will not only enhance the body of academic literature on cybersecurity but also stimulate discussion on the dynamic nature of vulnerability assessment and the continuous need for refinement in scoring methodologies. The findings could inform curriculum development in cybersecurity-related programs, encouraging a deeper engagement with the practical challenges and nuances of vulnerability assessment. Finally, the research will underscore the importance of keeping alongside developments in cybersecurity standards and practices, reinforcing the value of continuous learning and adaptability in the field.

### **Timeline/Plan of Work**

* **May 17 - May 31:** Literature review and initial data collection
* **June 1 - June 15:** Data analysis and historical review of CVE scoring changes
* **June 16 - June 30:** Conducting interviews with cybersecurity professionals
* **July 1 - July 15:** Comparative analysis and drafting the final report
* **July 16 - July 19:** Finalizing the report and preparing the poster presentation

**Literature Cited**

Ragan, S. (2018). Congress pushes MITRE to fix CVE program, suggests regular reviews and stable funding. *CSO (Online),*

Ruohonen, J. (2019). A look at the time delays in CVSS vulnerability scoring. *Applied Computing & Informatics*, *15*(2), 129–135. <https://doi.org/10.1016/j.aci.2017.12.002>

Mell, Peter., Kent, K. (Karen A., & Romanosky, Sasha. (2007). *The Common Vulnerability Scoring System (CVSS) and its applicability to Federal agency systems*. U.S. Dept. of Commerce, National Institute of Standards and Technology.

Wunder, J., Kurtz, A., Eichenmüller, C., Gassmann, F., & Benenson, Z. (2023). Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. *arXiv.Org*. https://doi.org/10.48550/arxiv.2308.15259

Houmb, S. H., Franqueira, V. N. L., & Engum, E. A. (2010). Quantifying security risk level from CVSS estimates of frequency and impact. *The Journal of Systems and Software*, *83*(9), 1622–1634. https://doi.org/10.1016/j.jss.2009.08.023