M8 Project Deliverable 4

Project Recap and Lessons Learned:

Common software weaknesses in CISAs Known Exploitable Catalog

**Project Background**

For this project, I analyzed data from three key sources in the cybersecurity field: the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the Massachusetts Institute of Technology Research and Engineering (MITRE). Cybersecurity specific terms such as Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and Common Vulnerability Scoring System (CVSS) will be frequently used. A brief description of each is as follows:

- CVEs are managed by NIST and provide a public method of sharing information about specific cybersecurity vulnerabilities.

- The CWEs database is managed by MITRE and is a category system for types of hardware and software weaknesses and vulnerabilities.

- CVSS is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way, as determined by the Forum of Incident Response and Security Teams (FIRST).

The primary aim of my project was to explore how CISA's catalog of known exploited vulnerabilities correlates with the information published in NIST and MITRE databases. I specifically wanted to determine if *certain software weaknesses, as defined by CWEs, are more prevalent within CISA's known exploitable catalog than others. If so what implications arise about commonly exploited software weaknesses, and are specific venders or products more frequently associated with certain CWEs?* This catalog is a crucial collection of vulnerabilities frequently targeted by malicious cyber actors and it holds significant importance for federal enterprises. Under operational directives, Federal Civilian Executive Branch agencies (FCEB) are mandated to address vulnerabilities listed in this catalog by prescribed due dates (Cybersecurity & Infrastructure Security Agency). To understand the relationship between these databases, I developed and deployed several Python3 scripts, linked in appendix A, which produced an enriched known exploitable catalog. This enriched data set could potentially guide future defense strategies and FCEB cybersecurity policy-making efforts.

**Project Approach and Initial Hypothesis**

The hypothesis at the core of my project revolved around the exploration of an existing dataset, CISA's known exploitable catalog, which initially lacked crucial CWE information. The primary tool for data extraction, correlation, and enrichment were my aforementioned Python scripts. I aimed to augment the known exploitable catalogs CVEs with corresponding CVSS scores and CWE IDs. In this phase, I faced challenges such as handling negative 'timeToFix' values in CISA's catalog, linked to retroactive CVE additions, and the necessity of converting CVSSv2 scores to CVSSv3.1 due to version inconsistencies. A significant concern was the high number of 'none' entries in the CWE column, which I addressed using my cybersecurity engineering experience, reducing the count from 90 to 13. The data preparation involved rigorous cleaning and processing, propelled by my python3 scripts and Linux terminal commands, after which my analysis primarily relied on histograms and heatmaps for visualizing the distribution of CWEs across different vendors.

**Analysis:**

The analysis revealed a marked prevalence of CWEs related to privilege management and input validation, with Microsoft products showing a notably higher count of known vulnerabilities, especially in privilege management areas. My analysis yielded several key findings, including a marked prevalence of CWEs related to privilege management and input validation with Microsoft products showing a notably higher count of known vulnerabilities. This was particularly evident in areas of privilege management. The following histograms provided clear insights into the frequency and distribution of various CWEs, while the heatmap detailed how these vulnerabilities spread across products from top vendors like Microsoft. The results effectively supported my initial hypothesis, demonstrating a distinct correlation between certain software weaknesses and their prevalence in CISA's known exploitable catalog, with particular implications for vendors like Microsoft.A graph of a number of people

Description automatically generated with medium confidence

Figure 1: Top ten CWEs in enriched CISA known exploitable catalog. Generated using Excel (Nov 2023)

Figure 1 The top ten most occurring CWEs in the enriched CISA data set. This specifically highlights the top ten most frequent CWEs. The top three CWEs in the data set map to “Improper Privilege Management’, ‘Input Validation’, and ‘Memory Buffer Overflow’, respectively. This suggests that the most common software weaknesses within the dataset are related to privilege management and input validation. It is important for organizations to properly secure privileges and properly validate input because these are common initial attack vectors used by attackers.

A graph with numbers and a bar

Description automatically generated with medium confidence

Figure 2: Top ten vendors in enriched CISA known exploitable catalog. Generated using Excel (Nov 2023)

Figure 2: The top ten venders within the data set. This chart reiterates that Microsoft products have the most occurrences of known vulnerabilities, followed by a steep drop-off for other vendors like Apple, Cisco, and Adobe. This reinforces the prominence of Microsoft products within the data set.

A chart of a table

Description automatically generated with medium confidence

Figure 3: Heatmap of CWE occurrences for top vendors. Generated using python script in appendix a (Nov 2023)

Figure 3: Maps are useful for displaying the context of which data exist in. Maps of all types are useful at simplifying complexity and allow readers to better visualize the relationships between data. The color contrasts clearly draw the reader's attention to the outliners in the data and can efficiently point out relationships. Figure 3 cross-references the top vendors with the prevalence of different CWEs in their products. The colors indicate the count of occurrences, with darker colors (deep blue, green) indicating higher counts. Microsoft has a significant concentration of CWE-269, which indicates improper privilege management as a pervasive software weakness in Microsoft products listed in CISAs known exploitable catalog.

**Results and Conclusions:**

My analysis and visualizations substantiate my initial hypothesis: *certain software weaknesses, as defined by CWEs, are indeed more prevalent within CISA's known exploitable database*. Notably, Microsoft products stood out with a higher frequency of known vulnerabilities, particularly those related to improper privilege management. This aligns with Microsoft's extensive market presence, making its products a common target in cybersecurity attacks.

While cybersecurity vulnerabilities are a widespread concern, certain weaknesses and products are disproportionately affected. This revelation is not only significant for understanding current cybersecurity landscapes, but also serves as guidance for future security measures. Specifically, it underscores the necessity for organizations, particularly Federal Civilian Executive Branch agencies (FCEBs), to adopt a more focused and robust approach to their cybersecurity strategies. To enhance security postures effectively, organizations should adopt comprehensive cybersecurity practices that hinder threat actors use of novel CVEs. This includes conducting thorough auditing, enforcing the principle of least privilege, and implementing defense in depth. Prioritizing the protection of high-value assets and processes, coupled with regular updates to business continuity and disaster recovery plans, are also essential steps in this direction. Furthermore, my analysis highlights the importance of proactive security measures. The implementation of robust auditing mechanisms and advanced analytical tools like User and Entity Behavior Analytics (UEBA) can significantly mitigate risks associated with the highest occurring CWE, improper privilege management. These tools, using machine learning and statistical analysis, can detect anomalous behaviors indicative of CVEs that attack account privileges, including novel attack vectors that may not yet be widely recognized.

In conclusion, this project has not only validated a key hypothesis concerning the prevalence of specific software weaknesses in CISA's known exploitable catalog but has also provided valuable insights into the nature of these vulnerabilities. The findings serve as a crucial resource for organizations in fortifying their defenses against the most exploited weaknesses. As the cybersecurity landscape continues to evolve, such insights will be instrumental in shaping more resilient and adaptive cybersecurity strategies for the future. Future research could extend this knowledge by investigating targeted mitigation strategies for each of the top ten CWEs identified to create more resilient and robust cybersecurity practices.

**Work Cited**

Cybersecurity & Infrastructure Security Agency. (n.d.). Known exploited vulnerabilities catalog.CISA. Retrieved from <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

**Appendixes:**

**Appendix A: Scrape and Parse from the web**

All scripts: <https://github.com/blugo2/AIT-664/tree/main>