**Root Cause Mapping Working Group**

**Meeting Notes**

**July 17, 2024**

**Agenda:**

1. **Preview 2024 CWE Top 25 Strategy**
2. **New mapping notes flow diagrams**
3. **Presentation by Chris Madden on Applying LLMs for CWE Assignment**

**Meeting Notes:**

**CWE Top 25 with Connor Mullally**

* **Previously discussed the prospect of changing the methodology, but now there’s a more concrete plan.**
  + **In previous years, the Top 25 analysis used the past two years of NVD data. The CWE team conducted independent analysis on thousands of CVE records.**
  + **There were difficulties with the lack of information and missing CVE descriptions. Certain companies can also choose to restrict the level of detail used to describe vulnerabilities for various reasons.**
* **Changes to the Methodology**
  + To use the past year of NVD data which will ultimately reduce the overall data set. (Has yet to be decided.)
  + To present CVE records back to CNAs to improve or correct mappings with the use of the internal keyword matcher and analysis scripts.
  + CNAs give more insight into their products to provide the best mappings available.
* **How to Present Remapping Data** 
  + How do we present this remapping data back to the CNAs?
    - Option 1. Use the text file format.
      * Not sure how digestible this is. It currently works internally.
    - Option 2. Use an excel file with one CVE per row that can be filled out by a CNA.
      * CVEs with multiple weaknesses would have multiple rows shown.
* **2024 CWE Top 25 – Considerations**
  + **Will CNAs have the capacity and willingness to help with mapping analysis?**
  + **How to ensure overall mapping accuracy/quality?**
    - **There’s a heavy reliance on CNAs being accurate in their analysis.**
    - **I.e.: handling conflicting/problematic mappings**
    - **Aiming for base-level weaknesses**
  + **Potential for 2024 list to be considerably different than previous, depending on community participation.**
    - **Having used the same methodology over the last 5/6 years, changes in the list are mostly accounted for in the data. Because the methodology will be different this year, any changes in the list will have to also take into account the differences in the methodology and could lead to difficulties drawing comparisons to previous years.**
  + **Possibilities of sharing mapping changes publicly for education and propagating lessons learned.**
* **Mapping Notes – New Flow Diagram**
  + **New in CWE 4.15 – Image for CWE-1420: Exposure of Sensitive Information during Transient Execution**
    - **To help with weakness related transient execution; helps them determine which one to use.**
    - **Useful to include in the mapping notes to help people with transient execution.**
* **Other CWEs to Consider in the Future**
  + **CWE-77: Command Injection**
    - **Will likely be a candidate for a diagram.**
    - **Most useful at the base or class level to identify the correct child to map from a higher level.**
  + **What CWEs do the group struggle with creating specific mappings?**
  + **Other Ideas**
    - **CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer**
    - **CWE-284: Improper Access Control**
* **Chris Madden Presentation**
  + **Spoke on leveraging AI to improve and to identify CWE for assignment to vulnerabilities. He presented two examples, simple and complex, to show how AI will provide suggestions and reference examples.**
  + **Simple refinements and confidence intervals can be made and updated as needed.**
  + **Members are encouraged to explore the resources presented:** 
    - **https://cybersecai.github.io/Vulnrichment/Vulnrichment/**
    - **https://cybersecai.github.io/NotebookLM/NotebookLM\_Cwe/**