CWE User Experience Working Group Meeting

August 30, 2023

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
  - CWE Element/Information Presentation
  - Grouping CWEs
  - CSV Download Colon Issue
  - Open Discussion
- **Reminders and Adjourn**

UEWG: Purpose

- **Mission:** Identifying areas where CWE content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them

- **Periodic reporting of activities to CWE Board**
  - (next quarterly Board meeting TBD Q3-2023)

- **Please solicit participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

- **CWE UEWG Meeting frequency**

  - Meetings have been changed and are now set to occur on the last Wednesday of the month

- **The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org**

Topic 1

CWE Element / Information Presentation

Chris Coffin

CWE Element/Information Presentation

- **When a user visits a CWE, what elements or information should be they be presented with first and in what format?**

- **The custom filters are a step in this direction and help users focus on the elements that are important to them**

- **Should a default view of CWE elements be created that focuses on just the right amount of information and ordering of elements?**

- **Could diagrams or graphics help understanding of weakness information and concepts?**

CWE Element/Information Presentation – Current Operational View

CWE-787: Out-of-bounds Write

Weakness ID: 787
Abstraction: Base
Structure: Simple

View customized information: | Conceptual | **Operational** | Mapping Friendly | Complete | Custom |

▼ Description

The product writes data past the end, or before the beginning, of the intended buffer.

▼ Extended Description

Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.

▼ Alternate Terms

Memory Corruption: Often used to describe the consequences of writing to memory outside the bounds of a buffer, or to memory that is invalid, when the root cause is something other than a sequential copy of excessive data from a fixed starting location. This may include issues such as incorrect pointer arithmetic, accessing invalid pointers due to incomplete initialization or memory release, etc.

▼ Relationships

ⓘ ▼ **Relevant to the view "Research Concepts" (CWE-1000)**

Nature	Type	ID	Name
ChildOf	🅖	119	Improper Restriction of Operations within the Bounds of a Memory Buffer
ParentOf	🅥	121	Stack-based Buffer Overflow
ParentOf	🅥	122	Heap-based Buffer Overflow
ParentOf	🅑	123	Write-what-where Condition
ParentOf	🅑	124	Buffer Underwrite ('Buffer Underflow')
CanFollow	🅑	822	Untrusted Pointer Dereference
CanFollow	🅑	823	Use of Out-of-range Pointer Offset
CanFollow	🅑	824	Access of Uninitialized Pointer

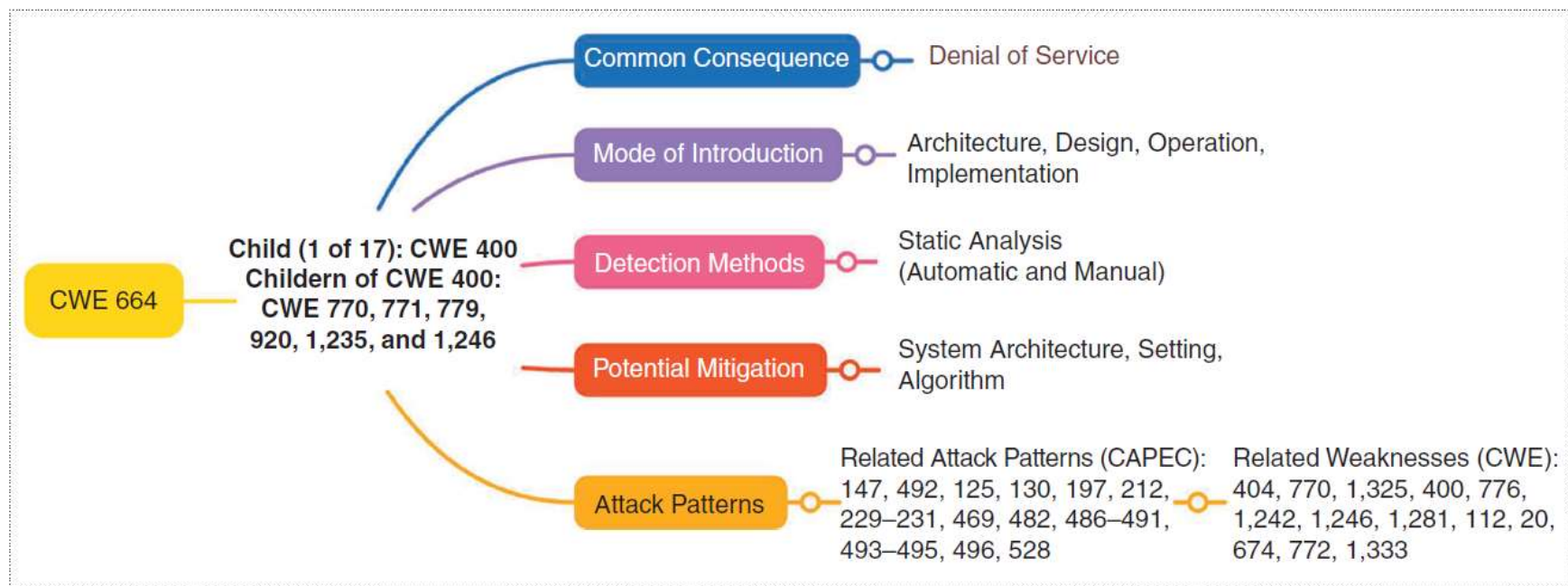# CWE Element/Information Presentation – A Graphical Representation of CWE

Figure 2. A partial analysis of CWE 664.

- Example from "Toward Common Weakness Enumerations in Industrial Control Systems," Co-published by the IEEE Computer and Reliability Societies, **https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10194510**

CWE Element/Information Presentation – Questions and Possible Next Steps

- **Who is the audience? Are we aiming at new, experienced, or all users?**

- **What CWE elements and information are most important to these users?**
    - Should these be the first things presented on any weakness page?

- **Should a graphical representation of the CWE information be investigated and/or created?**

- **Possible activity**
    - Volunteer to create a new weakness entry page structure for an existing weakness that improves user understandability and presents the most important information
    - CWE team will propose ideas for next meeting; other volunteers?

Topic 2

Grouping CWEs

Alec Summers

Grouping CWEs

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a

- **CWE entries are currently "grouped" in different ways to provide useful subsets of the CWE corpus for different purposes:**

  - Views: a subset of CWE entries that provides a way of examining CWE content. The two main view structures are Slices (flat lists) and Graphs (containing relationships between entries), examples include:

    - CWE-1194: Hardware Design

    - CWE-699: Software Development

    - CWE-1400: Comprehensive Categorization for Software Assurance Trends

    - CWE-1003: Weaknesses for Simplified Mapping of Published Vulnerabilities (NVD)

  - Categories: a CWE entry that contains a set of other entries that share a common characteristic. A category is not a weakness, but rather a structural item that helps users find weaknesses that share the stated common characteristic.

    - CWE-1199: General Circuit and Logic Design Concerns

  - ~ Overall Hierarchy

    - CWE-1000: Research Concepts contains all CWE entries in one hierarchical structure

Grouping CWEs, cont.

- **What groupings are most useful to new or casual CWE users? Experienced users?**

- **How can groupings be better presented/discovered/identified to the user?**

- **Should new users be guided to groupings of CWEs for learning about CWE? (e.g., links in user stories)**

- **Are there additional groupings that we are missing? Too many?**

Topic 3

CSV Download Colon Issue

David Rothenberg

CSV Single Colon Separators Within Column Data

- **A double colon is used to separate csv fields/columns data, while a single colon is used to separate multi-value data within fields/columns**

- **The Observed Examples field contains Reference and link data that includes a url in some cases (colon within "http://...")**

- **Should a note be added to the download data that warns the user of this, or should we look into an alternative separator?**

- **Example taken from CWE - CWE-41: Improper Resolution of Path Equivalence (4.12) (mitre.org)**

  - ::REFERENCE:CVE-2000-1114:DESCRIPTION:Source code disclosure using trailing dot:LINK:https://www.cve.org/CVERecord?id=CVE-2000-1114::REFERENCE:CVE-2002-1986:DESCRIPTION:Source code disclosure using trailing

Topic 4

Open Discussion

Chris Coffin

Miscellaneous Topics

- **Other thoughts or topics?**

Next Meeting – September 27 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

Backups

CWE User Pain Points

- **Pain point topics that the group is aware of or would like to discuss**

- **For those on the call, what were your biggest questions or concerns when beginning to use CWE?**

- **Are there common questions that CWE users have that are not covered in the current FAQ?**

- **Other potential opportunities:**
  - Features we could expand or improve to make CWE consumption easier?
  - Maybe engage the community in one or more ways to solicit this kind of feedback (see topic #3)

- **Other thoughts?**

Community Engagement Strategy

- **Develop a strategy for engaging the CWE user community for feedback**

- **What are the best methods to query the community on topics such as the pain points covered in topic #2**

- **What communication methods should be employed?**
  - E.g., polls, emails, web, social media

- **Should we target specific user types?**

- **Other thoughts?**

CWE Video Tips Series

- **Current video ideas:**
  - How to search CWE for a weakness
  - How to display only the information that you need with presentation filters
  - What is a weakness (vs a vulnerability)
  - How are weaknesses organized
  - What is a category (how is it different than a pillar)
  - What are views
  - How and why to use the research view
  - Use cases for CWE (could user stories be used?)
  - How do I submit an idea for a new weakness
  - How can I improve the quality of existing weaknesses

New to CWE – Future Content

- **The New to CWE content audience is different from what has been catered to previously**

- **The audience is the casual or new user to CWE or even the manager who makes security funding decisions**

- **The team has previously drafted material for the New to CWE audience that covers the CWE hierarchy**
  - Not yet released material
  - Do members agree that this topic should be covered for New to CWE?

- **Are there other topics that UEWG members feel strongly about or believe should be covered given the intended audience?**

- **Should there be a close coupling of the topics covered here with the CWE Video Tips series?**

CWE Naming and Vulnerability Mapping

- **Being thinking about solutions for common and well-known issues surrounding use of CWE names and how to more easily map vulnerabilities to CWEs**

- **Current CWE structure is difficult to understand and use**

- **Community needs better root cause information for vulnerabilities**

- **Does CWE naming need a change or update to support easier mapping?**

  - Remove CWE names for Views and/or Categories?

  - New naming that embeds a structure (e.g., CWE-1234-1)