**Introduction**

Organizations want assurance that the software products they acquire and develop are free of known types of security flaws. Today, high-quality tools and services for finding security flaws and weaknesses in code are new and the question of which tool/service is appropriate/better for a particular job is hard to answer given the lack of structure and definition in the code assessment industry. The Common Weakness Enumeration (CWE) was created specifically to address these problems.

**What Is CWE?**

Targeted to developers and security practitioners, CWE is a formal list of software weaknesses, idiosyncrasies, faults, and flaws created to:

- Serve as a common language for describing the source code, software design, or software architecture causes of software security vulnerabilities.
- Serve as a standard measuring stick for software security tools targeting these issues.
- Provide a common baseline standard for identification, mitigation, and prevention of these weaknesses.

MITRE began working on the issue of categorizing software weaknesses as early 1999 when it launched the Common Vulnerabilities and Exposures (CVE) List. As part of the development of CVE during the last 5+ years MITRE's CVE Team developed a preliminary classification and categorization of vulnerabilities, attacks, faults, and other concepts to help define common software weaknesses.

However, while sufficient for CVE those groupings were too rough to be used to identify and categorize the functionality offered within the offerings of the code security assessment industry. To be useful to these types of tools and the work they do some additional fidelity and succinctness were needed, as were additional details and description for each of the different nodes and groupings such as the effects, behaviors, and implementation details, etc.

To do this MITRE took a first cut at revising the internal CVE category work for usage in the code assessment industry in 2005 as part of MITRE's participation in the U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD)-sponsored National Institute of Technology (NIST) Software Assurance Metrics and Tool Evaluation (SAMATE) project. Our resulting work, entitled Preliminary List Of Vulnerability Examples for Researchers (PLOVER), has 300 types of flaws mapped from over 1,500 diverse, real-world examples of vulnerabilities in commercial and open source products, identified by their CVE name.

The next step was to combine PLOVER with other established groupings of software flaws. The first draft, which merges the items from PLOVER, CLASP, and the Seven Pernicious Kingdoms and others, is now available as the CWE list. The CWE List and its classification taxonomy will be refined and expanded and different views of the CWE list will also be established which will cut through the CWE list by scoping it to specific languages, frameworks, platforms, and machine architectures.

All are welcome to comment, contribute, and engage with the CWE effort. Please visit the site and participate.