Common Weakness Scoring System — CWSS™

Scoring the Severity of Software Weaknesses

CWSS is a mechanism for scoring the severity of Common Weakness Enumeration (CWE™) entries discovered in an enterprise's software applications, especially when used in conjunction with the Common Weakness Risk Analysis Framework (CWRAF™).

CWSS can also be used by individual developers to prioritize unfixed weaknesses within their own software.

Challenge

When a security analysis of a software application is performed, such as when using an automated code assessment tool, developers often face hundreds or thousands of individual findings for individual weaknesses that are identified in their code. In certain circumstances, a software weakness can lead to an exploitable vulnerability. For example, a buffer overflow weakness might arise from an input routine where the programmer does not properly validate the length of an input buffer. This weakness only contributes to a vulnerability if the input can be influenced by a malicious party, and if that malicious input can inserted into a buffer that is smaller than the malicious input.

Due to the high volume of reported weakness findings, developers are forced to prioritize which issues they should investigate and fix first. Similarly, when assessing design and architecture choices and their associated weaknesses, there needs to be a method for prioritizing them relative to each other and with the other issues in the application. Finally, software consumers want to know what issues they should worry about versus others, and what to ask about to get a more secure product from their vendors and suppliers.

Further complicating the problem, the importance of a weakness usually depends on the business or mission needs that the software is supporting, the kinds of technologies in use, and the threat environment.

In short, people need to be able to reason and communicate about the relative importance of different weaknesses. While various scoring methods are used today, they are either ad hoc or inappropriate for use against the evaluation of software security.

Solution

CWSS provides a mechanism for scoring weaknesses in a consistent, flexible, open manner while enabling an organization to reflect the context of their business domain(s). It is a collaborative, community-based effort that is addressing the needs of stakeholders across government, academia, and industry. CWSS is a part of the project, co-sponsored by the Software Assurance program in the office of Cybersecurity and Communications of the U.S. Department of Homeland Security (DHS).

CWSS:

- Provides a common framework for prioritizing security errors ("weaknesses") that are discovered in software applications
- Provides a quantitative measurement of the unfixed weaknesses that are present within a software application
- Can be used by developers to prioritize unfixed weaknesses within their own software
- In conjunction with CWRAF, can be used by consumers to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance.

Learn More – https://cwe.mitre.org/cwss

CWSS™

cwe.mitre.org/cwss

The MITRE Corporation maintains CWSS on the Common Weakness Enumeration (CWE™) website and provides impartial technical guidance to the CWSS community throughout the process to ensure CWSS serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org
MITRE

Common Weakness Risk Analysis Framework — CWRAF™

Prioritizing the Severity of Software Weaknesses in Your Own Organization

CWRAF is a way for organizations to apply the Common Weakness Scoring System (CWSS™) using specialized scenarios, or "vignettes," in order to prioritize those Common Weakness Enumeration (CWE™) entries that are most relevant to their own businesses, missions, and deployed technologies.

CWRAF provides a framework for scoring software weaknesses in a consistent, flexible, open manner, while accommodating context of an organization's business domain(s). It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry. CWRAF is a part of the Common Weakness Enumeration (CWE™) project, co-sponsored by the Software Assurance program in the office of Cybersecurity and Communications of the U.S. Department of Homeland Security (DHS).

CWRAF benefits:

- Includes a mechanism for measuring risk of security-relevant software development errors ("weaknesses") in a way that is closely linked with the potential impact to an organization's business or mission.
- Supports the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the organization's business or mission.
- Can be used by organizations in conjunction with CWSS to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance.
- Leverages the construct in CWE's Common Consequences information, where all CWEs, if manifested in an exploitable manner, result in the attacker being able to cause one or more of the following technical impacts: modify data; read data; DoS: unreliable execution; DoS: resource consumption; execute unauthorized code or commands; gain privileges /assume identity; bypass protection mechanism; and hide activities.

Vignettes Explained

CWRAF and CWSS allow users to rank classes of weaknesses independent of any particular software package, in order to prioritize them relative to each other (e.g., "buffer overflows are higher priority than memory leaks"). This method of prioritization, sometimes referred to as a "Top-N list," is used by the CWE/SANS Top 25, OWASP Top Ten, and similar efforts. CWRAF and CWSS allow users to create their own custom Top-N lists.

Within CWRAF, a vignette provides a shareable, formalized way to define a particular environment or operational context, i.e., the role that software plays within that environment, and an organization's priorities with respect to software security of that piece of software. It identifies essential resources and capabilities, as well as their importance relative to security principles such as confidentiality, integrity, and availability.

Vignettes allow CWSS to support diverse audiences who may have different requirements for how to prioritize weaknesses. CWSS scoring can occur within the context of a vignette.

There are currently 23 vignettes that are being actively developed for CWRAF within the categories, or "domains," of Banking/Finance, Chemical, e-Commerce, Emergency Services, Energy, e-Voting, Human Resources, National Defense, Public Health, Social Media, and Telecommunications. The CWRAF community will help to refine these and develop others over time including for Food & Water, Manufacturing, Homeland Security, Government (other), Teleworking, and Shipping/Transportation. Feedback is welcome.

Learn More - https://cwe.mitre.org/cwraf

CWRAF™

cwe.mitre.org/cwraf

The MITRE Corporation maintains CWRAF on the Common Weakness Enumeration (CWE™) website and provides impartial technical guidance to the CWRAF community throughout the process to ensure CWRAF serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org
MITRE