Common Weakness Enumeration (CWE)

Return to Glossary

Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weakness types that have security ramifications. “Weaknesses” are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack. The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of **CWEs**.

Targeted at both the development and security practitioner communities, the main goal of **CWE** is to stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate the most common mistakes before products are delivered. Ultimately, use of **CWE** helps prevent the kinds of security vulnerabilities that have plagued the software and hardware industries and put enterprises at risk.

CWE helps developers and security practitioners to:

- Describe and discuss software and hardware weaknesses in a common language.
- Check for weaknesses in existing software and hardware products.
- Evaluate coverage of tools targeting these weaknesses.
- Leverage a common baseline standard for weakness identification, mitigation, and prevention efforts.
- Prevent software and hardware vulnerabilities prior to deployment.

Source: https://cwe.mitre.org/about/index.html