ISO/IEC JTC 1/SC 22/OWGV N 0066

Proposal to the ISO/IEC Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use

Date	11 April 2007
Contributed by	Larry Wagoner
Original file name	sc22_proposal.doc
Notes	

Proposal to the ISO/IEC Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use

Submitted by Larry Wagoner

In order to focus on the most usable and commonly understandable standard, we must tie to other standards. Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org) is a standardized dictionary of names for vulnerabilities. It is a community wide effort with representatives from commercial security organizations, government, and academia. CVE has been very successful in creating a standardized vocabulary for communicating information about vulnerabilities.

Common Weakness Enumeration (CWE) (http://cwe.mitre.org) is accomplishing a similar goal for software weaknesses. CWE is targeted at security developers and practitioners and is creating a common language for describing software security weaknesses in architecture, design or code. Many organizations have already declared their intent to be CWE compatible. CWE is not a mature product, but is improving considerably with each iteration.

CWE can be viewed as a dictionary, a classification tree, a pdf file, an XML file or an XSD schema. CWE has a high degree of granularity. For instance, there are 11 different kinds of buffer errors (stack based or heap based buffer overflows) that ultimately lead to 46 different types of buffer errors to include XSS and SQL injection (types of string errors that are types of buffer errors).

Within the CWE dictionary, there are several fields for each entry including an ID number, description, observed examples and applicable platforms. Applicable platforms states which languages the weakness can occur in. CWE contains weaknesses that are very common both in occurrence and exploitation to the very obscure and rarely, if ever, exploited.

There are several items that I propose related to CWE:

1). That we state any and all vulnerabilities in CWE language using CWE IDs and terminology.
2). That we select some reasonable number of the vulnerabilities to be addressed in our standard. We could probably cover a large number of vulnerabilities by selecting 75-100 of the items from CWE. This would cover a large percentage of real world vulnerabilities.

Advantages to the proposals:

1). We will be speaking the language that is being adopted by many commercial security organizations, government and academia.
2). We will be leveraging the work that has been done on the CWE. Although not mature, CWE is a reasonable basis in its present form.