ISO/IEC JTC 1/SC 22/OWGV N 0068

Proposal to the ISO/IEC Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use: Vulnerabilities to Address in CWE - Part 3

Date	23 April 2007
Contributed by	Larry Wagoner
Original file name	sc22_proposal_part3.pdf
Notes	This is part 3 of a multi-part proposal. The other parts are N 0066 and N 0067.

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

Vulnerabilities to Address in CWE – Part 3

Submitted by Larry Wagoner

**NOTE: This is an attempt to illustrate the next needed step in the derivation of CWE entries to actionable secure coding guidance. This next step is not complete and needs additional work as only a select number of entries from Table 7 were used for illustration. **

The approach up to Table 7 was a mapping from the current most frequently exploited vulnerabilities to CWE entries. To make these items actionable to a software developer, recommendations must be made in terms that the developers can use. CERT has done a good job in their Secure Coding effort (www.cert.org/secure-coding). Table 8 is an illustration of how CWE leaf nodes and CERT Secure Coding Entries can be linked. The illustration uses the recommendations and rules for the C language as an example of the next step in the derivation. Note that though this is done only for the C language, the same recommendations and rule may be applicable to C++, Java and other languages. Also note that only a selected number of entries from Table 7 were mapped. Ultimately all of the entries in Table 7 will need to be mapped. Additional work will be needed to ensure the recommendation(s) or rule(s) in the CERT Secure Coding Entries cited are adequate to address the related CWE entry. It is clear that at least in some cases additional recommendations and rules will need to be created.

CWE Entry	***CERT Secure Coding Entry for C***
24. Path Issue - dot dot slash - '../filedir'	FIO02-A. Canonicalize filenames originating from untrusted sources
25. Path Issue - leading dot dot slash - '/../filedir'	FIO02-A. Canonicalize filenames originating from untrusted sources
26. Path Issue - leading directory dot dot slash - '/directory/../filename'	FIO02-A. Canonicalize filenames originating from untrusted sources
37. Path Issue - slash absolute path - /absolute/pathname/here	FIO05-A. Identify files using multiple file attributes
38. Path Issue - backslash absolute path - \absolute\pathname\here	FIO05-A. Identify files using multiple file attributes
39. Path Issue - drive letter or Windows volume - 'C:dirname'	FIO05-A. Identify files using multiple file attributes

CWE Entry	*CERT Secure Coding Entry for C*
62. UNIX Hard Link	FIO05-A. Identify files using multiple file attributes FIO07-A. Do not create temporary files in shared directories
64. Windows Shortcut Following (.LNK)	FIO05-A. Identify files using multiple file attributes
65. Windows Hard Link	FIO05-A. Identify files using multiple file attributes FIO07-A. Do not create temporary files in shared directories
192. Integer Coercion Error	INT02-A. Understand integer conversion rules Int11-A. Be careful converting small signed integers to larger unsigned integers Int35-C. Ensure that integer conversions do not result in lost or misinterpreted data ** many other INT recommendations/rules
197. Numeric Truncation Error	INT02-A. Understand integer conversion rules ** many other INT recommendations/rules
231. Extra Value Error	
476. Null Dereference	(can be/sort of) DCL30-C. Do not refer to an object outside of its lifetime Need additional recommendation/rules
365. Race Condition in Switch	MSC06-A. Avoid race conditions with shared data FIO31-C. Avoid race conditions while checking for the existence of a symbolic link Need additional recommendation/rules
368. Context Switching Race Condition	MSC06-A. Avoid race conditions with shared data Need additional recommendation/rules
415. Double Free	DCL30-C. Do not refer to an object outside of its lifetime
416. Use after Free	DCL30-C. Do not refer to an object outside of its lifetime
129. Unchecked Array Indexing	ARR30-C. Guarantee that array indices are within the valid range
550. Information Leak Through Server Error Message	Need recommendation/rules (or is this a design issue?)
215. Information Leak through Debug Information	Need recommendation/rules (or is this a design issue?)
219. Sensitive Data Under Web Root	Likely only a design issue

CWE Entry	*CERT Secure Coding Entry for C*
230. Missing Value Error	FIO04-A. Detect and handle input output errors Need additional recommendation/rules
256. Plaintext Storage	
257. Storing Passwords in a Recoverable Format	Need recommendation/rules
250. Often Misused: Privilege Management	Need recommendation/rules
266. Incorrect Privilege Assignment	Need recommendation/rules
267. Unsafe Privilege	Need recommendation/rules
268. Privilege Chaining	Need recommendation/rules
257. Storing Passwords in a Recoverable Format	FIO39-C. Create temporary files securely Need additional recommendation/rules
259. Hard-coded Password	Need recommendation/rules (or is this a design issue?)
401. Memory Leak	Need recommendation/rules
591. Memory Locking	Need recommendation/rules
446. User Interface Inconsistency	Likely only a design issue
570. Expression is Always False	MSC00-A. Compile cleanly at high warning levels Need additional recommendation/rules
571. Expression is Always True	MSC00-A. Compile cleanly at high warning levels Need additional recommendation/rules
563. Unused Variable	MSC00-A. Compile cleanly at high warning levels

Table 1Mapping some entries from CWE (Table 7) to CERT Secure Coding Entry