ISO/IEC JTC 1/SC 22/OWGV N 0112

Proposed organization of vulnerability descriptions (with annotations from OWGV Meeting #7)

Date	14 December 2007
Contributed by	Secretary
Original file name	
Notes	Annotated version of N0109

Document N0109 was considered at Meeting #7 of the OWGV. Consideration resulted in annotations shown in the form of markups.

Formatted: Indent: Left: 18 pt

We made some decisions about the use of this outline:

- The outline would be used to structure a clause that would provide a topical outline of the vulnerabilities treated in the document and would provide pointers to the descriptions themselves that are organized in a flat manner in a distinct clause. (However, the descriptions might be sorted in the same order as the outline.)
- Any particular vulnerability may be placed at more than one point in the outline.
- The outline will be used to categorize the vulnerabilities by adding the appropriate subclause number(s) to the category section of each vulnerability description.
- The purpose of the outline is to help the reader find a small selection of descriptions relevant to the problem they are interested in.

Formatted: Bulleted + Level: 1 + Aligned at: 36 pt + Tab after: 54 pt + Indent at: 54 pt

Consideration of OWGV meeting #7 also resulted in a suggestions for changing the outline. They are interspersed below:

Formatted: Indent: Left: 18 pt

1. Human Factors
    1. BRS-PENDING-leveraging-human-experience
2. Environment
    1. XYN-PENDING-privilege-management
    2. XYO-PENDING-privilege-sandbox-issues
    3. interactions with environment
3. Core Language Issues
    1. BQF-PENDING-unspecified-behavior
    2. EWF-PENDING-undefined-behavior
    3. FAB-PENDING-implementation-defined-behavior
    4. MEM-PENDING-deprecated-features
4. Documentation
5. Preprocessor
    1. NMP-PENDING-preprocessor-directives
6. Declarations and Definitions
    1. NAI-PENDING-choice of clear names
    2. XYR-PENDING-unused-variable
    3. YOW-PENDING-identifier-name-reuse
7. Types
        1. IHN-PENDING-strong-typing
        2. STR-PENDING-bit-representations
    1. Constants
    2. ~~Integers~~
    3. Floating point
    4. PLF-PENDING-floating-point-arithmetic (should be indented under floating point)

Formatted: Bullets and Numbering

   5. Integers
      1. XYE-PENDING-integer-coercion-errors
   6. Characters and strings
   7. Arrays
      1. XYX-PENDING-boundary-beginning-violation
      2. XYZ-PENDING-unchecked-array-indexing
   8. Pointers (move to follow arrays and other structured types)
      1. HFC-PENDING-pointer-casting-and-pointer-type-changes
      2. RVG-PENDING-pointer-arithmetic
      3. XYH-PENDING-null-pointer-dereference
      4. XYK-PENDING-pointer-use-after-free
   9. Structures and Unions
   10. Vectors
   11. Enumerated Types (move to precede integer so that scalar types are first)
       1. CCB-PENDING-enumerator-issues
   12. Objects (promote to the top level)
       1. Templates/Generics (promote to the top level)
          1. SYM-PENDING-templates-and-generics
          2. STL (CERT)
       2. Inheritance
   13. Sets and other containers

Formatted: Bullets and Numbering

8. Initialization
   1. LAV-PENDING-initialization-of-variables
9. Type Conversions/Limits
   1. XYY-PENDING-wrap-around-error
   2. XZI-PENDING-sign-extension-error
   3. XYF-PENDING-numeric-truncation-error
10. Operators/Expressions
    1. JCW-PENDING-operator-precedence
    2. SAM-PENDING-order-of-evaluation
    3. KOA-PENDING-likely-incorrect-expressions
    4. XYQ-PENDING-expression-issues
    5. MTW-PENDING-associativity
11. Control Flow (add a subcategory for exceptions)
    1. Case/Switch Statements (change name to conditionals)
       1. CLL-PENDING-switch-statements-and-static-analysis
       2. XYI-OUT-race-condition-in-switch
       3. XYJ-OUT-context-switching-race-condition
       4. EOJ-PENDING-demarcation-of-control-flow
    2. Loops
       1. TMP-PENDING-loop-control-variables
    3. Subroutines (Functions, Procedures, Subprograms)(might be dealt with as process abstraction to also include methods)
       1. EWD-PENDING-control-structure
       2. CSJ-PENDING-passing-parameters-and-return-values
       3. DCM-PENDING-dangling-references-to-stack-frames
       4. XZA-OUT-unsafe-function-call
       5. XYW-PENDING-buffer-overflow-in-stack (group with arrays)
       6. XZB-PENDING-buffer-overflow-in-heap (group with arrays)
       7. XZM-PENDING-missing-parameter-error
       8. GDL-PENDING-recursion
       9. XYS-PENDING-process-control
       10. XYG-PENDING-value-problems
           1. NZN-PENDING-returning-error-status
    4. Termination Strategy
       1. REU-PENDING-termination-strategy
12. External interfaces
    1. Memory Management

1. AMV-PENDING-overlapping-memory
2. XYL-PENDING-memory-leak
3. XZX-PENDING-memory-locking
4. XZP-PENDING-resource-exhaustion

   2. Input
      1. RST-PENDING-injection
      2. XYT-PENDING-cross-site Scripting
      3. XZQ-PENDING-unquoted-search-path-or-element
      4. XZR-PENDING-improperly-verified-signature
      5. XZL-PENDING-discrepancy-information-leak
   3. Output
      1. XZK-PENDING-sensitive-information-uncleared-before-use
   4. Libraries
      1. TRJ-PENDING-use-of-libraries
      2. NYY-PENDING-dynamically-linked-code-and-self-modifying-code
   5. Files
      1. EWR-PENDING-path-traversal
   6. Signals

13. External issues
    1. Portable Code
14. Miscellaneous
    1. XZH-PENDING-off-by-one-error
    2. XZS-PENDING-missing-required-cryptographic-step
    3. Authentication
       1. XYM-PENDING-insufficiently-protected-credentials
       2. XZN-PENDING-missing-or-inconsistent-access-control
       3. XZO-PENDING-authentication-logic-error
       4. XYP-PENDING-hard-coded-password