ISO/IEC JTC 1/SC 22/OWGV N 0117

Outline of Vulnerability Descriptions, 24 December 2007 (with assignments for update)

Date	24 December 2007
Contributed by	John Benito, editor
Original file name	vulnerability_outline_assignment.doc
Notes	Replaces N0112

Outline of Vulnerability Descriptions, 24 December 2007

(with assignments for update)

1. Human Factors
    1.1. BRS-PENDING-leveraging-human-experience (Plum)
2. Environment
    2.1. XYN-PENDING-privilege-management
    2.2. XYO-PENDING-privilege-sandbox-issues
    2.3. Interactions with environment
3. Core Language Issues
    3.1. BQF-PENDING-unspecified-behavior (Jones)
    3.2. EWF-PENDING-undefined-behavior (Jones)
    3.3. FAB-PENDING-implementation-defined-behavior (Jones)
    3.4. MEM-PENDING-deprecated-features (Wagoner)
4. Documentation
5. Preprocessor
    5.1. NMP-PENDING-preprocessor-directives (Benito)
6. Declarations and Definitions
    6.1. NAI-PENDING-choice-of-clear-names (Wagoner)
    6.2. AJN-PENDING-choice-of-filenames-and-other-external-identifiers (Wagoner)
    6.3. XYR-PENDING-unused-variable (Ploedereder)
    6.4. YOW-PENDING-identifier-name-reuse (Seacord)
7. Types
    7.1. Representation
        7.1.1. IHN-PENDING-strong-typing (Moore)
        7.1.2. STR-PENDING-bit-representations (Moore)
    7.2. Constants
    7.3. Floating point
        7.3.1. PLF-PENDING-floating-point-arithmetic (Wagoner)
    7.4. Enumerated Types
        7.4.1. CCB-PENDING-enumerator-issues (Michell)
    7.5. Integers
        7.5.1. XYE-PENDING-integer-coercion-errors (Seacord)
    7.6. Characters and strings
    7.7. Arrays
        7.7.1. XYX-PENDING-boundary-beginning-violation (Jones)
        7.7.2. XYZ-PENDING-unchecked-array-indexing
        7.7.3. XYW-PENDING-buffer-overflow-in-stack
        7.7.4. XZB-PENDING-buffer-overflow-in-heap
    7.8. Structures and Unions
    7.9. Pointers
        7.9.1. HFC-PENDING-pointer-casting-and-pointer-type-changes (Plum)
        7.9.2. RVG-PENDING-pointer-arithmetic (Benito)
        7.9.3. XYH-PENDING-null-pointer-dereference
        7.9.4. XYK-PENDING-pointer-use-after-free (Ploedereder)
    7.10. Vectors
8. Objects
9. Templates/Generics

9.1. SYM-PENDING-templates-and-generics (Pygott)
9.2. STL (CERT)
9.2.1. Inheritance
9.3. Sets and other containers
10. Initialization
10.1. LAV-PENDING-initialization-of-variables (Michell)
11. Type Conversions/Limits
11.1. XYY-PENDING-wrap-around-error (Nagle)
11.2. XZI-PENDING-sign-extension-error (Plum)
11.3. XYF-PENDING-numeric-truncation-error (Nagle)
12. Operators/Expressions
12.1. JCW-PENDING-operator-precedence (Plum)
12.2. SAM-PENDING-order-of-evaluation (Plum)
12.3. KOA-PENDING-likely-incorrect-expressions (Wagoner)
12.4. XYQ-PENDING-expression-issues (Pygott)
12.5. MTW-PENDING-associativity (Plum)
13. Control Flow
13.1. Conditional Statements
13.1.1. CLL-PENDING-switch-statements-and-static-analysis (Plum)
13.1.2. XYI-OUT-race-condition-in-switch
13.1.3. XYJ-OUT-context-switching-race-condition
13.1.4. EOJ-PENDING-demarcation-of-control-flow (Plum)
13.2. Loops
13.2.1. TEX-PENDING-loop-control-variables (Jones)
13.3. Subroutines (Functions, Procedures, Subprograms)
13.3.1. EWD-PENDING-control-structure (Benito)
13.3.2. CSJ-PENDING-passing-parameters-and-return-values (Moore)
13.3.3. DCM-PENDING-dangling-references-to-stack-frames (Ploedereder)
13.3.4. XZA-OUT-unsafe-function-call
13.3.5. OTR-PENDING-subprogram-signature-mismatch (Moore)
13.3.6. GDL-PENDING-recursion (Moore)
13.3.7. XYS-PENDING-process-control
13.3.8. NZN-PENDING-returning-error-status (Moore)
13.4. Termination Strategy
13.4.1. REU-PENDING-termination-strategy (Wagoner)
13.5. Exceptions
14. External interfaces
14.1. Memory Management
14.1.1. AMV-PENDING-overlapping-memory (Moore)
14.1.2. XYL-PENDING-memory-leak (Michell)
14.1.3. XZX-PENDING-memory-locking
14.1.4. XZP-PENDING-resource-exhaustion
14.2. Input
14.2.1. RST-PENDING-injection
14.2.2. XYT-PENDING-cross-site Scripting
14.2.3. XZQ-PENDING-unquoted-search-path-or-element
14.2.4. XZR-PENDING-improperly-verified-signature
14.2.5. XZL-PENDING-discrepancy-information-leak
14.3. Output

14.3.1. XZK-PENDING-sensitive-information-uncleared-before-use
14.4. Libraries
14.4.1. TRJ-PENDING-use-of-libraries (Benito)
14.4.2. NYY-PENDING-dynamically-linked-code-and-self-modifying-code (Plum)
14.5. Files
14.5.1. EWR-PENDING-path-traversal
14.6. Signals
15. External issues
15.1. Portable Code
16. Miscellaneous
16.1. XZH-PENDING-off-by-one-error (Michell)
16.2. XZS-PENDING-missing-required-cryptographic-step
16.3. Authentication
16.3.1. XYM-PENDING-insufficiently-protected-credentials
16.3.2. XZN-PENDING-missing-or-inconsistent-access-control
16.3.3. XZO-PENDING-authentication-logic-error
16.3.4. XYP-PENDING-hard-coded-password (Pygott)