

# ISO/IEC JTC 1/SC 22/WG 23 N 0282

*Revised outline of vulnerabilities*

**Date** 16 September 2010  
**Contributed by** Jim Moore  
**Original file name**  
**Notes** Best viewed as “Final” rather than “Final showing markup”

## **D.1 Outline of Programming Language Vulnerabilities**

D.1.6. Types  
D.1.9. Type Conversions/Limits  
D.1.5. Declarations and Definitions  
D.1.10. Operators/Expressions  
D.1.11. Control Flow  
D.1.13.1. Memory Models  
D.1.7. Templates/Generics  
  
D.1.13.4. Libraries  
D.1.4. Pre-processor (rename as Macros)  
D.1.1 Language Specification Issues

## **D.2 Outline of Application Vulnerabilities**

D.1.3. Design Issues  
    D.1.3.5. [BVQ] Unspecified Functionality  
    D.1.6.1.3. [KLK] Distinguished Values in Data Types  
D.1.2. Environment  
    D.1.2.1. [XYN] Adherence to Least Privilege  
    D.1.2.2. [XYO] Privilege Sandbox Issues  
    D.1.2.3.1. [XYS] Executing or Loading Untrusted Code  
  
D.1.13. Resource Management  
    D.1.13.1. Memory Management  
        D.1.13.1.3. [XZX] Memory Locking  
        D.1.13.1.4. [XZP] Resource Exhaustion  
    D.1.13.2. Input  
        D.1.13.2.1. [RST] Injection  
        D.1.13.2.2. [XYT] Cross-site Scripting  
        D.1.13.2.3. [XZQ] Unquoted Search Path or Element

- D.1.13.2.4. [XZR] Improperly Verified Signature
- D.1.13.2.5. [XZL] Discrepancy Information Leak
- D.1.13.3. Output
  - D.1.13.3.1. [XZK] Sensitive Information Uncleared Before Use
- D.1.13.5. Files
  - D.1.13.5.1. [EWR] Path Traversal
- D.1.14. Flaws in Security Functions
  - D.1.14.1. [XZS] Missing Required Cryptographic Step
  - D.1.14.2. Authentication
    - D.1.14.2.1. [XYM] Insufficiently Protected Credentials
    - D.1.14.2.2. [XZN] Missing or Inconsistent Access Control
    - D.1.14.2.3. [XZO] Authentication Logic Error
    - D.1.14.2.4. [XYP] Hard-coded Password