

# ISO/IEC TR 24772:2010-10 (E)

Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use

---

<b>Contents</b>		Page
Foreword .....		vi
Introduction .....		vii
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions, symbols and conventions .....</b>	<b>1</b>
<b>3.1</b>	<b>Terms and definitions, symbols and conventions.....</b>	<b>1</b>
<b>3.2</b>	<b>Symbols and conventions.....</b>	<b>3</b>
<b>4</b>	<b>Basic Concepts .....</b>	<b>4</b>
<b>4.1</b>	<b>Not in Scope.....</b>	<b>4</b>
<b>4.2</b>	<b>Approach .....</b>	<b>4</b>
<b>4.3</b>	<b>Intended Audience.....</b>	<b>4</b>
<b>4.4</b>	<b>How to Use This Document .....</b>	<b>5</b>
<b>5</b>	<b>Vulnerability issues .....</b>	<b>8</b>
<b>5.1</b>	<b>Issues arising from incomplete or evolving language specifications .....</b>	<b>8</b>
<b>5.2</b>	<b>Issues arising from human cognitive limitations .....</b>	<b>11</b>
<b>5.3</b>	<b>Issues arising from a lack of predictable execution .....</b>	<b>12</b>
<b>5.4</b>	<b>Issues arising from the lack of portability and interoperability .....</b>	<b>12</b>
<b>5.5</b>	<b>Issues arising from inadequate language intrinsic support.....</b>	<b>13</b>
<b>5.6</b>	<b>Issues arising from language features prone to erroneous use.....</b>	<b>13</b>
<b>6</b>	<b>Programming Language Vulnerabilities .....</b>	<b>14</b>
<b>6.1</b>	<b>General .....</b>	<b>14</b>
<b>6.2</b>	<b>Obscure Language Features [BRS] .....</b>	<b>14</b>
<b>6.3</b>	<b>Unspecified Behaviour [BQF].....</b>	<b>15</b>
<b>6.4</b>	<b>Undefined Behaviour [EWF] .....</b>	<b>17</b>
<b>6.5</b>	<b>Implementation-defined Behaviour [FAB] .....</b>	<b>18</b>
<b>6.6</b>	<b>Deprecated Language Features [MEM].....</b>	<b>20</b>
<b>6.7</b>	<b>Pre-processor Directives [NMP].....</b>	<b>21</b>
<b>6.8</b>	<b>Choice of Clear Names [NAI].....</b>	<b>23</b>
<b>6.9</b>	<b>Choice of Filenames and other External Identifiers [AJN].....</b>	<b>25</b>
<b>6.10</b>	<b>Unused Variable [XYR] .....</b>	<b>26</b>
<b>6.11</b>	<b>Identifier Name Reuse [YOW] .....</b>	<b>27</b>
<b>6.12</b>	<b>Namespace Issues [BJL].....</b>	<b>30</b>
<b>6.13</b>	<b>Type System [IHN].....</b>	<b>31</b>
<b>6.14</b>	<b>Bit Representations [STR].....</b>	<b>34</b>
<b>6.15</b>	<b>Floating-point Arithmetic [PLF] .....</b>	<b>35</b>
<b>6.16</b>	<b>Enumerator Issues [CCB] .....</b>	<b>38</b>
<b>6.17</b>	<b>Numeric Conversion Errors [FLC] .....</b>	<b>40</b>

6.18	String Termination [CJM] .....	42
6.19	Boundary Beginning Violation [XYX] .....	43
6.20	Unchecked Array Indexing [XYZ] .....	44
6.21	Unchecked Array Copying [XYW] .....	46
6.22	Buffer Overflow [XZB].....	47
6.23	Pointer Casting and Pointer Type Changes [HFC].....	49
6.24	Pointer Arithmetic [RVG] .....	50
6.25	Null Pointer Dereference [XYH] .....	51
6.26	Dangling Reference to Heap [XYK] .....	52
6.27	Templates and Generics [SYM] .....	54
6.28	Inheritance [RIP].....	56
6.29	Initialization of Variables [LAV].....	57
6.30	Wrap-around Error [XYY] .....	59
6.31	Sign Extension Error [XZI] .....	60
6.32	Operator Precedence/Order of Evaluation [JCW].....	61
6.33	Side-effects and Order of Evaluation [SAM] .....	63
6.34	Likely Incorrect Expression [KOA] .....	64
6.35	Dead and Deactivated Code [XYQ].....	66
6.36	Switch Statements and Static Analysis [CLL] .....	68
6.37	Demarcation of Control Flow [EOJ] .....	69
6.38	Loop Control Variables [TEX] .....	70
6.39	Off-by-one Error [XZH].....	71
6.40	Structured Programming [EWD] .....	73
6.41	Passing Parameters and Return Values [CSJ].....	74
6.42	Dangling References to Stack Frames [DCM].....	77
6.43	Subprogram Signature Mismatch [OTR].....	79
6.44	Recursion [GDL].....	80
6.45	Returning Error Status [NZN] .....	81
6.46	Termination Strategy [REU] .....	84
6.47	Extra Intrinsic [LRM].....	85
6.48	Type-breaking Reinterpretation of Data [AMV] .....	87
6.49	Memory Leak [XYL].....	89
6.50	Argument Passing to Library Functions [TRJ].....	90
6.51	Dynamically-linked Code and Self-modifying Code [NYY].....	91
6.52	Library Signature [NSQ] .....	92
6.53	Unanticipated Exceptions from Library Routines [HJW] .....	93
7	Application Vulnerabilities.....	95
7.1	Adherence to Least Privilege [XYN] .....	95
7.2	Privilege Sandbox Issues [XYO] .....	95
7.3	Executing or Loading Untrusted Code [XYS] .....	97
7.4	Unspecified Functionality [BVQ] .....	98
7.5	Distinguished Values in Data Types [KLK].....	99
7.6	Memory Locking [XZX].....	100

7.7	Resource Exhaustion [XZP] .....	101
7.8	Injection [RST].....	102
7.9	Cross-site Scripting [XYT].....	105
7.10	Unquoted Search Path or Element [XZQ].....	108
7.11	Improperly Verified Signature [XZR] .....	108
7.12	Discrepancy Information Leak [XZL] .....	109
7.13	Sensitive Information Uncleared Before Release [XZK].....	110
7.14	Path Traversal [EWR] .....	111
7.15	Missing Required Cryptographic Step [XZS] .....	113
7.16	Insufficiently Protected Credentials [XYM] .....	113
7.17	Missing or Inconsistent Access Control [XZN] .....	114
7.18	Authentication Logic Error [XZO] .....	115
7.19	Hard-coded Password [XYP] .....	117
Annex A (informative) Guideline Selection Process.....		118
A.1	Selection Process.....	118
A.2	Cost/Benefit Analysis .....	118
A.3	Documenting of the selection process .....	119
Annex B (informative) Template for use in proposing programming language vulnerabilities .....		120
B.1	6.<x> <short title> [<unique immutable identifier>].....	120
Annex C (informative) Template for use in proposing application vulnerabilities .....		122
C.1	7.<x> <short title> [<unique immutable identifier>] .....	122
Annex D (informative) Vulnerability Outline and List .....		123
D.1	Vulnerability Outline .....	123
D.2	Vulnerability List .....	125
Annex E (informative) Language Specific Vulnerability Template .....		127
E.1	<language>.1 Identification of standards.....	127
E.2	<language>.2 General terminology and concepts .....	127
E.3	<language>.<x> <Vulnerability Name> [<3 letter tag>] .....	127
Bibliography .....		129