

# ISO/IEC TR 24772-3:2020-05 (E)

## Programming languages - Guidance to avoiding vulnerabilities in programming languages - Part 3: C

---

<b>Contents</b>		<b>Page</b>
Foreword .....		vii
Introduction .....		viii
<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</b> .....	<b>1</b>
<b>4</b>	<b>Language concepts</b> .....	<b>2</b>
<b>5</b>	<b>Avoiding programming language vulnerabilities in C</b> .....	<b>2</b>
<b>6</b>	<b>Specific guidance for C vulnerabilities</b> .....	<b>3</b>
6.1	General .....	3
6.2	Type system [IHN] .....	4
6.2.1	Applicability to language .....	4
6.2.2	Guidance to language users .....	5
6.3	Bit representations [STR] .....	5
6.3.1	Applicability to language .....	5
6.3.2	Guidance to language users .....	5
6.4	Floating-point arithmetic [PLF] .....	6
6.4.1	Applicability to language .....	6
6.4.2	Guidance to language users .....	6
6.5	Enumerator issues [CCB] .....	6
6.5.1	Applicability to language .....	6
6.5.2	Guidance to language users .....	7
6.6	Conversion errors [FLC] .....	8
6.6.1	Applicability to language .....	8
6.6.2	Guidance to language users .....	9
6.7	String termination [CJM] .....	10
6.7.1	Applicability to language .....	10
6.7.2	Guidance to language users .....	10
6.8	Buffer boundary violation (buffer overflow) [HCB] .....	10
6.8.1	Applicability to language .....	10
6.8.2	Guidance to language users .....	11
6.9	Unchecked array indexing [XYZ] .....	11
6.9.1	Applicability to language .....	11
6.9.2	Guidance to language users .....	12
6.10	Unchecked array copying [XYW] .....	12
6.10.1	Applicability to language .....	12
6.10.2	Guidance to language users .....	12
6.11	Pointer type conversions [HFC] .....	13
6.11.1	Applicability to language .....	13
6.11.2	Guidance to language users .....	13
6.12	Pointer arithmetic [RVG] .....	13
6.12.1	Applicability to language .....	13
6.12.2	Guidance to language users .....	14
6.13	Null pointer dereference [XYH] .....	14
6.13.1	Applicability to language .....	14
6.13.2	Guidance to language users .....	14
6.14	Dangling reference to heap [XYK] .....	15
6.14.1	Applicability to language .....	15
6.14.2	Guidance to language users .....	15

6.15	Arithmetic wrap-around error [FIF]	16
6.15.1	Applicability to language	16
6.15.2	Guidance to language users	16
6.16	Using shift operations for multiplication and division [PIK]	17
6.16.1	Applicability to language	17
6.16.2	Guidance to language users	17
6.17	Choice of clear names [NAI]	17
6.17.1	Applicability to language	17
6.17.2	Guidance to language users	17
6.18	Dead store [WXQ]	18
6.18.1	Applicability to language	18
6.18.2	Guidance to language users	18
6.19	Unused variable [YZS]	18
6.19.1	Applicability to language	18
6.19.2	Guidance to language users	18
6.20	Identifier name reuse [YOW]	18
6.20.1	Applicability to language	18
6.20.2	Guidance to language users	19
6.21	Namespace issues [BJL]	19
6.21.1	Applicability to language	19
6.22	Initialization of variables [LAV]	19
6.22.1	Applicability to language	19
6.22.2	Guidance to language users	19
6.23	Operator precedence and associativity [JCW]	19
6.23.1	Applicability to language	19
6.23.2	Guidance to language users	20
6.24	Side-effects and order of evaluation of operands [SAM]	20
6.24.1	Applicability to language	20
6.24.2	Guidance to language users	20
6.25	Likely incorrect expression [KOA]	21
6.25.1	Applicability to language	21
6.25.2	Guidance to language users	21
6.26	Dead and deactivated code [XYQ]	22
6.26.1	Applicability to language	22
6.26.2	Guidance to language users	22
6.27	Switch statements and static analysis [CLL]	22
6.27.1	Applicability to language	22
6.27.2	Guidance to language users	23
6.28	Demarcation of control flow [EOJ]	23
6.28.1	Applicability to language	23
6.28.2	Guidance to language users	23
6.29	Loop control variables [TEX]	24
6.29.1	Applicability to language	24
6.29.2	Guidance to language users	24
6.30	Off-by-one error [XZH]	25
6.30.1	Applicability to language	25
6.30.2	Guidance to language users	25
6.31	Unstructured programming [EWD]	25
6.31.1	Applicability to language	25
6.31.2	Guidance to language users	25
6.32	Passing parameters and return values [CSJ]	26
6.32.1	Applicability to language	26
6.32.2	Guidance to language users	26
6.33	Dangling references to stack frames [DCM]	27
6.33.1	Applicability to language	27
6.33.2	Guidance to language users	27
6.34	Subprogram signature mismatch [OTR]	27
6.34.1	Applicability to language	27
6.34.2	Guidance to language users	28
6.35	Recursion [GDL]	28
6.35.1	Applicability to language	28
6.35.2	Guidance to language users	28

6.36	Ignored error status and unhandled exceptions [OYB]	28
6.36.1	Applicability to language	28
6.36.2	Guidance to language users	28
6.37	Type-breaking reinterpretation of data [AMV]	29
6.37.1	Applicability to language	29
6.37.2	Guidance to language users	29
6.38	Deep vs. shallow copying [YAN]	29
6.38.1	Applicability to language	29
6.38.2	Guidance to language users	29
6.39	Memory leaks and heap fragmentation [XYL]	30
6.39.1	Applicability to language	30
6.39.2	Guidance to language users	30
6.40	Templates and generics [SYM]	30
6.41	Inheritance [RIP]	30
6.42	Violations of the Liskov substitution principle or the contract model [BLP]	30
6.43	Redispatching [PPH]	30
6.44	Polymorphic variables [BKK]	30
6.45	Extra intrinsics [LRM]	30
6.46	Argument passing to library functions [TRJ]	30
6.46.1	Applicability to language	30
6.46.2	Guidance to language users	31
6.47	Inter-language calling [DJS]	31
6.47.1	Applicability to language	31
6.47.2	Guidance to language users	31
6.48	Dynamically linked code and self-modifying code [NYY]	31
6.48.1	Applicability to language	31
6.48.2	Guidance to language users	32
6.49	Library signature [NSQ]	32
6.49.1	Applicability to language	32
6.49.2	Guidance to language users	32
6.50	Unanticipated exceptions from library routines [HJW]	32
6.51	Pre-processor directives [NMP]	32
6.51.1	Applicability to language	32
6.51.2	Guidance to language users	33
6.52	Suppression of language-defined run-time checking [MXB]	33
6.53	Provision of inherently unsafe operations [SKL]	33
6.53.1	Applicability to language	33
6.53.2	Guidance to language users	33
6.54	Obscure language features [BRS]	34
6.54.1	Applicability of language	34
6.54.2	Guidance to language users	34
6.55	Unspecified behaviour [BQF]	34
6.55.1	Applicability of language	34
6.55.2	Guidance to language users	34
6.56	Undefined behaviour [EWF]	34
6.56.1	Applicability to language	34
6.56.2	Guidance to language users	35
6.57	Implementation-defined behaviour [FAB]	35
6.57.1	Applicability to language	35
6.57.2	Guidance to language users	35
6.58	Deprecated language features [MEM]	36
6.58.1	Applicability to language	36
6.58.2	Guidance to language users	36
6.59	Concurrency — Activation [CGA]	36
6.59.1	Applicability to language	36
6.59.2	Guidance to language users	36
6.60	Concurrency — Directed termination [CGT]	36
6.61	Concurrent data access [CGX]	36

6.61.1	Applicability to language .....	36
6.61.2	Guidance to language users.....	37
6.62	Concurrency — Premature termination [CGS] .....	37
6.62.1	Applicability to language .....	37
6.62.2	Guidance to language users.....	37
6.63	Lock protocol errors [CGM] .....	37
6.63.1	Applicability to language .....	37
6.63.2	Guidance to language users.....	37
6.64	Reliance on external format strings.....	37
6.64.1	Applicability to language .....	37
6.64.2	Guidance to language users.....	37
<b>Bibliography</b> .....		<b>38</b>
<b>Index</b> .....		<b>39</b>