



## Parasoft Support for CWE in C/C++ - C/C++test 9.x

The following table shows how Mitre's Common Weakness Enumeration (CWE) maps to Parasoft's static analysis rules for C/C++.

CWE ID	CWE Name/Description	Parasoft Rule ID(s)
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').	BD-SECURITY-TDFNAMES
CWE-23	Relative Path Traversal.	BD-SECURITY-TDFNAMES
CWE-36	Absolute Path Traversal.	BD-SECURITY-TDFNAMES
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	SECURITY-17, SECURITY-18
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').	BD-SECURITY-TDSQL
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').	BD-PB-OVERFFMT, BD-PB-OVERFNZT, BD-PB-OVERFWR, BD-SECURITY-OVERFWR
CWE-121	Stack-based Buffer Overflow.	BD-PB-ARRAY, BD-PB-OVERFWR, BD-SECURITY-ARRAY
CWE-122	Heap-based Buffer Overflow.	BD-PB-ARRAY, BD-PB-OVERFWR, BD-SECURITY-ARRAY
CWE-124	Buffer Underwrite ('Buffer Underflow').	BD-PB-ARRAY, BD-PB-OVERFWR, BD-SECURITY-ARRAY
CWE-126	Buffer Over-read.	BD-PB-ARRAY, BD-SECURITY-ARRAY
CWE-127	Buffer Under-read.	BD-PB-ARRAY, BD-PB-OVERFRD, BD-SECURITY-ARRAY
CWE-131	Incorrect Calculation of Buffer Size.	BD-PB-ARRAY, BD-PB-OVERFRD, BD-SECURITY-ARRAY, BD-SECURITY-OVERFRD, MRM-45
CWE-134	Use of Externally-Controlled Format String.	SECURITY-05, SECURITY-08, SECURITY-36
CWE-190	Integer Overflow or Wraparound.	BD-SECURITY-INTOVERF, MISRA-051
CWE-242	Use of Inherently Dangerous Function.	SECURITY-16
CWE-252	Unchecked Return Value.	MISRA2004-16_10
CWE-327	Use of a Broken or Risky Cryptographic Algorithm.	SECURITY-02, SECURITY-28, SECURITY-37
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).	SECURITY-02

CWE-369	Divide By Zero.	BD-PB-ZERO
CWE-396	Declaration of Catch for Generic Exception.	EXCEPT-17
CWE-398	Indicator of Poor Code Quality.	MISRA2004-14_2, OPT-32, OPT-35
CWE-400	Uncontrolled Resource Consumption ('Resource Exhaustion').	SECURITY-38
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak').	BD-RES-LEAKS, MRM-18, MRM-19, MRM-33, OOP-24
CWE-415	Double Free.	BD-RES-FREE, MRM-49
CWE-416	Use After Free.	BD-RES-FREE, OOP-34
CWE-440	Expected Behavior Violation.	EXCEPT-14
CWE-457	Use of Uninitialized Variable.	BD-PB-NOTINIT, INIT-06
CWE-467	Use of sizeof() on a Pointer Type.	PB-32
CWE-468	Incorrect Pointer Scaling.	MISRA-101
CWE-469	Use of Pointer Subtraction to Determine Size.	MISRA2004-17_2
CWE-476	NULL Pointer Dereference.	BD-PB-NP
CWE-478	Missing Default Case in Switch Statement.	CODSTA-35
CWE-480	Use of Incorrect Operator.	MISRA2004-16_9
CWE-481	Assigning instead of Comparing.	PB-35
CWE-482	Comparing instead of Assigning.	MISRA2004-14_2
CWE-483	Incorrect Block Delimitation.	MISRA2004-14_9
CWE-484	Omitted Break Statement in Switch.	MISRA2004-15_2
CWE-500	Public Static Field Not Marked Final.	OOP-18
CWE-511	Logic/Time Bomb.	SECURITY-01
CWE-547	Use of Hard-coded, Security-relevant Constants.	CODSTA-29
CWE-561	Dead Code.	BD-PB-SWITCH, MISRA2004-14_1_a, MISRA2004-14_1_b, MISRA2004-14_1_c, MISRA2004-14_1_d, MISRA2004-14_1_e, MISRA2004-14_1_f, OPT-30
CWE-562	Return of Stack Variable Address.	CODSTA-30, MISRA2004-17_6_a, MISRA2004-17_6_b
CWE-563	Assignment to Variable without Use ('Unused Variable').	OPT-03, OPT-35, OPT-06
CWE-570	Expression is Always False.	BD-PB-CC, MISRA2004-13_7_n
CWE-571	Expression is Always True.	BD-PB-CC, MISRA2004-13_7_n

CWE-587	Assignment of a Fixed Address to a Pointer.	MISRA2004-11_3_b
CWE-590	Free of Memory not on the Heap.	BD-RES-INVFREE
CWE-674	Uncontrolled Recursion.	MISRA2004-16_2
CWE-675	Duplicate Operations on Resource.	BD-RES-FREE
CWE-676	Use of Potentially Dangerous Function.	PB-37, SECURITY-11, SECURITY-12, SECURITY-13, SECURITY-14, SECURITY-16, SECURITY-22, SECURITY-30, SECURITY-31
CWE-680	Integer Overflow to Buffer Overflow.	BD-SECURITY-INTOVERF
CWE-685	Function Call With Incorrect Number of Arguments.	PB-50
CWE-688	Function Call With Incorrect Variable or Reference as Argument.	PB-45
CWE-690	Unchecked Return Value to NULL Pointer Dereference.	BD-PB-NP
CWE-758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior.	BD-PB-NOTINIT, MISRA2004-16_8
CWE-762	Mismatched Memory Management Routines.	BD-RES-LEAKS, MRM-06, MRM-35, MRM-36
CWE-773	Missing Reference to Active File Descriptor or Handle.	BD-RES-LEAKS
CWE-775	Missing Release of File Descriptor or Handle after Effective Lifetime.	BD-RES-LEAKS
CWE-789	Uncontrolled Memory Allocation.	BD-SECURITY-INTOVERF
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop').	CODSTA-82