



## Parasoft Support for CWE in C/C++ - C/C++test 10.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-20	Improper Input Validation.	SECURITY-38 BD-SECURITY-ARRAY SECURITY-36 BD-SECURITY-TDCMD BD-SECURITY-TDENV BD-SECURITY-TDFNAMES BD-SECURITY-TDSQL BD-PB-INTOVERTF
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-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	SECURITY-20
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection').	BD-SECURITY-TDCMD
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	BD-SECURITY-TDCMD BD-SECURITY-TDENV SECURITY-11 SECURITY-17 SECURITY-18
CWE-88	Argument Injection or Modification.	SECURITY-20
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').	BD-SECURITY-TDSQL
CWE-99	Improper Control of Resource Identifiers ('Resource Injection').	BD-SECURITY-ARRAY

CWE-114	Process Control.	BD-SECURITY-TDENV
CWE-118	Improper Access of Indexable Resource ('Range Error').	BD-SECURITY-OVERFFMT BD-SECURITY-OVERFRD
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer.	BD-SECURITY-OVERFFMT BD-SECURITY-OVERFRD BD-SECURITY-OVERFWR
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').	BD-PB-OVERFFMT BD-PB-OVERFNZT BD-PB-OVERFWR BD-SECURITY-BUFWRITE BD-SECURITY-OVERFFMT BD-SECURITY-OVERFWR CODSTA-143 BD-SECURITY-OVERFRD BD-SECURITY-OVERFWR BD-PB-OVERFRD BD-PB-OVERFWR CODSTA-144 CODSTA-145 MRM-45 BD-PB-OVERFWR
CWE-121	Stack-based Buffer Overflow.	MISRA2008-7_5_4 BD-SECURITY-OVERFRD BD-PB-OVERFWR BD-PB-ARRAY BD-PB-OVERFRD BD-SECURITY-ARRAY SECURITY-12
CWE-122	Heap-based Buffer Overflow.	BD-PB-OVERFWR BD-PB-ARRAY BD-SECURITY-ARRAY BD-PB-OVERFRD SECURITY-12
CWE-123	Write-what-where Condition.	SECURITY-36
CWE-124	Buffer Underwrite ('Buffer Underflow').	BD-PB-ARRAY BD-PB-OVERFARRAY
CWE-125	Out-of-bounds Read.	BD-PB-OVERFARRAY
CWE-126	Buffer Over-read.	BD-PB-OVERFRD BD-PB-ARRAY BD-SECURITY-ARRAY SECURITY-12

CWE-127	Buffer Under-read.	BD-PB-OVERFRD BD-PB-ARRAY BD-SECURITY-ARRAY SECURITY-12
CWE-128	Wrap-around Error.	JSF-203 MISRA-051
CWE-129	Improper Validation of Array Index.	BD-SECURITY-ARRAY
CWE-130	Improper Handling of Length Parameter Inconsistency .	BD-SECURITY-OVERFFMT
CWE-131	Incorrect Calculation of Buffer Size.	BD-PB-ARRAY BD-PB-OVERFRD BD-SECURITY-ARRAY BD-SECURITY-OVERFRD MRM-45
CWE-132	DEPRECATED (Duplicate): Miscalculated Null Termination.	BD-PB-NZTS CODSTA-144 CODSTA-145 PB-21
CWE-134	Use of Externally-Controlled Format String.	SECURITY-05 SECURITY-08 SECURITY-36
CWE-140	Improper Neutralization of Delimiters.	MISRA2008-16_2_4
CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences.	CODSTACPP-60
CWE-156	Improper Neutralization of Whitespace.	FORMAT-17
CWE-158	Improper Neutralization of Null Byte or NUL Character.	PB-21
CWE-170	Improper Null Termination.	BD-PB-NZTS CODSTA-144 CODSTA-145 PB-21 BD-SECURITY-OVERFRD BD-SECURITY-OVERFWR BD-PB-OVERFRD BD-PB-OVERFWR MRM-45 BD-PB-OVERFNZT

CWE-178	Improper Handling of Case Sensitivity.	SECURITY-03
CWE-188	Reliance on Data/Memory Layout.	MISRA2004-11_4 BD-PB-PTRARR
CWE-190	Integer Overflow or Wraparound.	BD-PB-INTOVERF BD-SECURITY-INTOVERF MISRA-051 PB-65 PB-65_b PB-66_a PB-66_b
CWE-191	Integer Underflow (Wrap or Wraparound).	BD-PB-INTOVERF PB-66_a PB-66_b
CWE-194	Unexpected Sign Extension.	BD-SECURITY-INTOVERF
CWE-195	Signed to Unsigned Conversion Error.	BD-SECURITY-INTOVERF MISRA2004-10_1_a MISRA2004-10_1_h
CWE-196	Unsigned to Signed Conversion Error.	BD-SECURITY-INTOVERF MISRA2004-10_1_a MISRA2004-10_1_h
CWE-197	Numeric Truncation Error.	CODSTA-146 JSF-182 BD-PB-CC MISRA2004-14_2 MISRA2004-13_7_ai MISRA2004-15_4 OPT-32 OPT-35 CODSTA-31
CWE-198	Use of Incorrect Byte Ordering.	PORT-03
CWE-221	Information Loss or Omission.	SECURITY-12 BD-SECURITY-OVERFWR BD-SECURITY-INTOVERF
CWE-223	Omission of Security-relevant Information.	SECURITY-14 SECURITY-15
CWE-224	Obscured Security-relevant Information by Alternate Name.	SECURITY-14 SECURITY-15
CWE-226	Sensitive Information Uncleared Before Release.	JSF-070.1 JSF-153
CWE-229	Improper Handling of Values.	JSF-108

CWE-231	Improper Handling of Extra Values.	BD-PB-OVERFFMT BD-PB-OVERFWR SECURITY-12
CWE-242	Use of Inherently Dangerous Function.	SECURITY-16 SECURITY-30 SECURITY-07 SECURITY-23
CWE-243	Creation of chroot Jail Without Changing Working Directory.	SECURITY-41
CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection').	MRM-46
CWE-248	Uncaught Exception.	EXCEPT-06
CWE-252	Unchecked Return Value.	BD-PB-CHECKRET BD-PB-CHECKRETGEN MISRA2004-16_10
CWE-253	Incorrect Check of Function Return Value.	BD-PB-CHECKRET BD-PB-CHECKRETGEN
CWE-261	Weak Cryptography for Passwords.	SECURITY-37
CWE-276	Incorrect Default Permissions.	BD-SECURITY-TDCMD
CWE-281	Improper Preservation of Permissions.	MRM-40_b
CWE-326	Inadequate Encryption Strength.	SECURITY-37
CWE-327	Use of a Broken or Risky Cryptographic Algorithm.	SECURITY-02 SECURITY-28 SECURITY-37
CWE-330	Use of Insufficiently Random Values.	SECURITY-28
CWE-332	Insufficient Entropy in PRNG.	SECURITY-28
CWE-334	Small Space of Random Values.	SECURITY-28
CWE-335	PRNG Seed Error.	SECURITY-28
CWE-336	Same Seed in PRNG.	SECURITY-28
CWE-337	Predictable Seed in PRNG.	SECURITY-28
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).	SECURITY-28 SECURITY-02
CWE-339	Small Seed Space in PRNG.	SECURITY-28

CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	SECURITY-19
CWE-365	Race Condition in Switch.	CODSTA-64
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition.	SECURITY-19
CWE-369	Divide By Zero.	BD-PB-ZERO
CWE-377	Insecure Temporary File.	SECURITY-23-2 SECURITY-39-3
CWE-378	Creation of Temporary File With Insecure Permissions.	SECURITY-23
CWE-379	Creation of Temporary File in Directory with Incorrect Permissions.	SECURITY-23
CWE-391	Unchecked Error Condition.	BD-PB-ERRNO
CWE-394	Unexpected Status Code or Return Value.	BD-PB-CHECKRET BD-PB-CHECKRETGEN
CWE-396	Declaration of Catch for Generic Exception.	EXCEPT-17
CWE-398	Indicator of Poor Code Quality.	BD-PB-CC MISRA2004-14_2 MISRA2004-13_7_ai MISRA2004-15_4 OPT-32 OPT-35 OPT-14 EXCEPT-02 NOP-24
CWE-400	Uncontrolled Resource Consumption ('Resource Exhaustion').	SECURITY-38 BD-SECURITY-ARRAY SECURITY-36 BD-SECURITY-TDCMD BD-SECURITY-TDENV BD-SECURITY-TDFNAMES BD-SECURITY-TDSQL BD-PB-INTOVERTF

CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak').	MRM-19 BD-RES-LEAKS MRM-18 MRM-33 OOP-24 BD-PB-CC OPT-32 BD-RES-INVFREE
CWE-404	Improper Resource Shutdown or Release.	BD-RES-LEAKS BD-RES-LEAKS BD-RES-STACKLIM-3
CWE-412	Unrestricted Externally Accessible Lock.	BD-TRS-MLOCK
CWE-415	Double Free.	BD-RES-FREE MRM-49
CWE-416	Use After Free.	BD-RES-FREE OOP-34 MRM-31
CWE-421	Race Condition During Access to Alternate Channel.	BD-SECURITY-TDCMD
CWE-426	Untrusted Search Path.	SECURITY-11
CWE-428	Unquoted Search Path or Element.	SECURITY-17 SECURITY-18
CWE-431	Missing Handler.	EXCEPT-06
CWE-432	Dangerous Signal Handler not Disabled During Sensitive Operations.	JSF-021 JSF-021_b
CWE-440	Expected Behavior Violation.	EXCEPT-14
CWE-448	Obsolete Feature in UI.	SECURITY-32
CWE-457	Use of Uninitialized Variable.	BD-PB-NOTINIT INIT-06 MISRA2004-13_7_ai
CWE-460	Improper Cleanup on Thrown Exception.	EXCEPT-04
CWE-466	Return of Pointer Value Outside of Expected Range.	BD-PB-ARRAY
CWE-467	Use of sizeof() on a Pointer Type.	MRM-45 PB-32
CWE-468	Incorrect Pointer Scaling.	BD-PB-ARRAY MISRA-101

CWE-469	Use of Pointer Subtraction to Determine Size.	MISRA2004-17_2
CWE-476	NULL Pointer Dereference.	BD-PB-NP BD-PB-DEREF
CWE-477	Use of Obsolete Functions.	BD-PB-DEREF
CWE-478	Missing Default Case in Switch Statement.	MISRA2012-RULE-16_4_a CODSTA-35
CWE-480	Use of Incorrect Operator.	BD-PB-CC MISRA2004-16_9
CWE-481	Assigning instead of Comparing.	MISRA2004-13_1 BD-PB-CC PB-35
CWE-482	Comparing instead of Assigning.	MISRA2004-14_2 BD-PB-CC
CWE-483	Incorrect Block Delimitation.	MISRA2004-14_9
CWE-484	Omitted Break Statement in Switch.	CODSTA-149 MISRA2004-15_2
CWE-497	Exposure of System Data to an Unauthorized Control Sphere.	SECURITY-03
CWE-500	Public Static Field Not Marked Final.	OOP-18
CWE-506	Embedded Malicious Code.	BD-PB-OVERFNZT
CWE-511	Logic/Time Bomb.	SECURITY-01
CWE-538	File and Directory Information Exposure.	BD-SECURITY-TDFNAMES
CWE-547	Use of Hard-coded, Security-relevant Constants.	CODSTA-29 PORT-03
CWE-548	Information Exposure Through Directory Listing.	SECURITY-23
CWE-550	Information Exposure Through Server Error Message.	SECURITY-15
CWE-552	Files or Directories Accessible to External Parties.	SECURITY-23



CWE-561	Dead Code.	BD-PB-CC 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 MISRA2004-14_1_g OPT-30
CWE-562	Return of Stack Variable Address.	MISRA2004-17_6_a MISRA2004-17_6_b CODSTA-30
CWE-563	Assignment to Variable without Use ('Unused Variable').	BD-PB-POVR BD-PB-VOVR OPT-03 OPT-05 OPT-06
CWE-570	Expression is Always False.	BD-PB-CC MISRA2004-13_7_ai
CWE-571	Expression is Always True.	BD-PB-CC MISRA2004-13_7_ai
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-597	Use of Wrong Operator in String Comparison.	CODSTA-148
CWE-628	Function Call with Incorrectly Specified Arguments.	MISRA2004-16_6
CWE-665	Improper Initialization.	BD-PB-CC OPT-32
CWE-670	Always-Incorrect Control Flow Implementation.	CODSTA-57
CWE-674	Uncontrolled Recursion.	MISRA2004-16_2
CWE-675	Duplicate Operations on Resource.	BD-RES-FREE

CWE-676	Use of Potentially Dangerous Function.	SECURITY-31 SECURITY-01 SECURITY-02 SECURITY-07 SECURITY-12 SECURITY-13 SECURITY-14 SECURITY-28 MISRA2008-18_0_5 PB-37 SECURITY-11 SECURITY-14 SECURITY-30 SECURITY-22 SECURITY-16
CWE-680	Integer Overflow to Buffer Overflow.	BD-PB-ARRAY BD-SECURITY-INTOVERF
CWE-681	Incorrect Conversion between Numeric Types.	MISRA2004-10_4
CWE-683	Function Call With Incorrect Order of Arguments.	PB-62 JSF-204.1_b JSF-204.1_c
CWE-685	Function Call With Incorrect Number of Arguments.	PB-50 MISRA2004-16_6
CWE-686	Function Call With Incorrect Argument Type.	PB-62 JSF-204.1_b JSF-204.1_c
CWE-688	Function Call With Incorrect Variable or Reference as Argument.	PB-45
CWE-690	Unchecked Return Value to NULL Pointer Dereference.	MRM-34 BD-PB-NP
CWE-694	Use of Multiple Resources with Duplicate Identifier.	CDD-002 CDD-003 CDD-004
CWE-704	Incorrect Type Conversion or Cast.	MISRA2004-10_1_b MISRA2004-10_2_a MISRA2004-11_4
CWE-705	Incorrect Control Flow Scoping.	BD-PB-CC

CWE-758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior.	BD-PB-NOTINIT MISRA2004-16_8
CWE-761	Free of Pointer not at Start of Buffer.	MISRA2004-17_4
CWE-762	Mismatched Memory Management Routines.	MRM-06 MRM-35 MRM-36 BD-RES-LEAKS
CWE-763	Release of Invalid Pointer or Reference.	BD-RES-INVFREE
CWE-764	Multiple Locks of a Critical Resource.	BD-TRS-DLOCK BD-TRS-LOCK
CWE-765	Multiple Unlocks of a Critical Resource.	BD-TRS-DLOCK
CWE-766	Critical Variable Declared Public.	OOP-18
CWE-767	Access to Critical Private Variable via Public Method.	OOP-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-783	Operator Precedence Logic Error.	CODSTA-97 MISRA2004-12_1_b
CWE-786	Access of Memory Location Before Start of Buffer.	BD-PB-OVERFRD BD-SECURITY-OVERFWR BD-PB-OVERFWR
CWE-787	Out-of-bounds Write.	BD-SECURITY-OVERFWR BD-PB-OVERFWR
CWE-788	Access of Memory Location After End of Buffer.	BD-PB-OVERFRD BD-SECURITY-OVERFWR BD-SECURITY-OVERFRD BD-PB-OVERFWR
CWE-789	Uncontrolled Memory Allocation.	BD-SECURITY-INTOVERF
CWE-805	Buffer Access with Incorrect Length Value.	BD-PB-ARRAY

CWE-806	Buffer Access Using Size of Source Buffer.	BD-PB-ARRAY
CWE-822	Untrusted Pointer Dereference.	PB-01-3
CWE-824	Access of Uninitialized Pointer.	INIT-04-2
CWE-825	Expired Pointer Dereference.	INIT-05-1
CWE-826	Premature Release of Resource During Expected Lifetime.	INIT-05-1
CWE-832	Unlock of a Resource that is not Locked.	BD-TRS-LOCK
CWE-833	Deadlock.	QT-08-3
CWE-834	Excessive Iteration.	CODSTA-83-3
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop').	CODSTA-82
CWE-908	Use of Uninitialized Resource.	JSF-142_b INIT-04
CWE-909	Missing Initialization of Resource.	BD-PB-NOTINIT
CWE-910	Use of Expired File Descriptor.	BD-RES-FREE
CWE-912	Hidden Functionality.	COMMENT-04