

DATASHEET

CWE Mapping - QAC++

CWE ID	CWE Text	QAC Rule Group ID	QAC Rule Text
CWE-014	Compiler Removal of Code to Clear Buffers	5.10	Redundancy
CWE-020	Improper Input Validation	5.5	Overflow and wraparound
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	5.6	Arrays
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	5.6	Arrays
CWE-121	Stack-based Buffer Overflow	5.6	Arrays
CWE-122	Heap-based Buffer Overflow	5.6	Arrays
CWE-124	Buffer Underwrite	5.6	Arrays
CWE-125	Out-of-bounds Read	5.6	Arrays
CWE-126	Buffer Over-read	5.6	Arrays
CWE-127	Buffer Under-read	5.6	Arrays
CWE-128	Wrap-around Error	5.5	Overflow and wraparound
CWE-129	Improper Validation of Array Index	5.6	Arrays
CWE-129	Improper Validation of Array Index	5.5	Overflow and wraparound
CWE-131	Incorrect Calculation of Buffer Size	5.6	Arrays
CWE-170	Improper NULL termination	5.6	Arrays
CWE-188	Reliance on Data/Memory Layout	6.4	Implementation Defined
CWE-188	Reliance on Data/Memory Layout	5.1	Conversion to Signed
CWE-188	Reliance on Data/Memory Layout	6.1	Portability Problems
CWE-188	Reliance on Data/Memory Layout	5.22	Preventive Measures
CWE-190	Integer Overflow or Wraparound	5.5	Overflow and wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)	5.5	Overflow and wraparound
CWE-192	Integer Coercion Error	5.1	Conversion to signed
CWE-192	Integer Coercion Error	5.2	Conversion to unsigned
CWE-193	Off-by-one Error	5.6	Arrays

CWE ID	CWE Text	QAC Rule Group ID	QAC Rule Text
CWE-194	Unexpected Sign Extension	5.2	Conversion to unsigned
CWE-195	Signed to Unsigned Conversion Error	5.2	Conversion to unsigned
CWE-196	Unsigned to Signed Conversion Error	5.1	Conversion to signed
CWE-197	Numeric Truncation Error	5.1	Conversion to signed
CWE-197	Numeric Truncation Error	5.2	Conversion to unsigned
CWE-248	Uncaught Exception	5.17	Serious Exception Problems
CWE-248	Uncaught Exception	5.21	Potential Exception Problems
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization	5.14	Serious Threading Issues
CWE-375	Returning a Mutable Object to an Untrusted Caller	5.22	Preventive Measures
CWE-375	Returning a Mutable Object to an Untrusted Caller	5.19	Potential Problems
CWE-397	Declaration of Throws for Generic Exception	8.3	Syntax Warnings
CWE-397	Declaration of Throws for Generic Exception	2.18	Functions
CWE-397	Declaration of Throws for Generic Exception	2.19	Identifiers
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	2.6	Arithmetic type - Integral promotion
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	5.16	Serious Resource Leaks
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	5.11	Resources
CWE-415	Double Free	5.11	Resources
CWE-416	User After Free	2.4	Arithmetic type - Casts
CWE-457	Use of Uninitialized Variable	5.9	Unset Data
CWE-457	Use of Uninitialized Variable	1.11	Arithmetic type - Implicit conversions
CWE-466	Return of Pointer Value Outside of Expected Range	5.6	Arrays
CWE-468	Incorrect Pointer Scaling	5.6	Arrays
CWE-468	Incorrect Pointer Scaling	5.7	Pointers
CWE-469	Use of Pointer Subtraction to Determine Size	5.7	Pointers
CWE-476	NULL Pointer Dereference	5.9	Null Pointers
CWE-478	Missing Default Case in Switch Statement	1.11	Arithmetic type - Implicit conversions
CWE-478	Missing Default Case in Switch Statement	1.3	Code Structure Standards
CWE-480	Use of Incorrect Operator	5.19	Potential Problems
CWE-480	Use of Incorrect Operator	2.18	Functions

CWE ID	CWE Text	QAC Rule Group ID	QAC Rule Text
CWE-480	Use of Incorrect Operator	1.11	Arithmetic type - Implicit conversions
CWE-481	Assigning instead of Comparing	1.11	Arithmetic type - Implicit conversions
CWE-482	Comparing instead of Assigning	2.18	Functions
CWE-483	Incorrect Block Delimitation	1.11	Arithmetic type - Implicit conversions
CWE-484	Omitted Break Statement in Switch	1.11	Arithmetic type - Implicit conversions
CWE-484	Omitted Break Statement in Switch	1.3	Code Structure Standards
CWE-493	Critical Public Variable Without Final Modifier	2.6	Arithmetic type - Integral promotion
CWE-495	Private Array-Typed Field Returned From A Public Method	5.22	Preventive Measures
CWE-495	Private Array-Typed Field Returned From A Public Method	5.19	Potential Problems
CWE-500	Public Static Field Not Marked Final	1.2	Declaration Standards
CWE-543	Use of Singleton Pattern W/ Synchronization in a Multithreaded Context	1.11	Arithmetic type - Implicit conversions
CWE-559	Often Misused: Arguments and Parameters	3.8	Functions
CWE-562	Return of Stack Variable Address	2.1	Maintenance Warnings
CWE-562	Return of Stack Variable Address	5.15	Serious Problems
CWE-562	Return of Stack Variable Address	5.19	Potential Problems
CWE-562	Return of Stack Variable Address	5.7	Pointers
CWE-587	Assignment of a Fixed Address to a Pointer	5.22	Preventative Measures
CWE-690	Unchecked Return Value to NULL Pointer Dereference	5.9	Null Pointers
CWE-704	Incorrect Type Conversion or Cast	2.4	Arithmetic type - Casts
CWE-704	Incorrect Type Conversion or Cast	5.1	Conversion to signed
CWE-704	Incorrect Type Conversion or Cast	5.2	Conversion to unsigned
CWE-704	Incorrect Type Conversion or Cast	3.3	Arithmetic type - Casts
CWE-704	Incorrect Type Conversion or Cast	5.19	Potential Problems
CWE-704	Incorrect Type Conversion or Cast	5.22	Preventative Measures
CWE-704	Incorrect Type Conversion or Cast	5.15	Serious Problems
CWE-704	Incorrect Type Conversion or Cast	8.4	Deprecated
CWE-704	Incorrect Type Conversion or Cast	2.13	Constants
CWE-704	Incorrect Type Conversion or Cast	2.25	Readability
CWE-704	Incorrect Type Conversion or Cast	6.4	Implementation Defined
CWE-704	Incorrect Type Conversion or Cast	1.11	Arithmetic type - Implicit conversions
CWE-704	Incorrect Type Conversion or Cast	2.1	Maintenance Warnings

CWE ID	CWE Text	QAC Rule Group ID	QAC Rule Text
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code	5.12	Control Flow
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code	5.10	Redundancy
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code	5.13	Invariant Operations
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code	2.1	Maintenance Warnings
CWE-762	Mismatched Memory Management Routines	5.11	Resources
CWE-766	Critical Variable Declared Public	1.2	Declaration Standards
CWE-767	Access to Critical Private Variable via Public Method	5.22	Preventative Measures
CWE-783	Operator Precedence Logic Error	2.1	Maintenance Warnings
CWE-805	Buffer Access with Incorrect Length Value	5.6	Arrays
CWE-806	Buffer Access with Incorrect Length Value	5.6	Arrays
CWE-839	Numeric Range Comparison Without Minimum Check	5.6	Arrays
CWE-839	Numeric Range Comparison Without Minimum Check	5.2	Conversion to unsigned
CWE-839	Numeric Range Comparison Without Minimum Check	5.6	Arrays
CWE-843	Access of Resource Using Incompatible Type	8.2	Semantic Warnings
CWE-843	Access of Resource Using Incompatible Type	1.3	Code Structure Standards
CWE-843	Access of Resource Using Incompatible Type	6.4	Implementation Defined
CWE-843	Access of Resource Using Incompatible Type	5.15	Serious Problems
CWE-910	Use of Expired File Descriptor	5.11	Resources
CWE-911	Improper Update of Reference Count	5.15	Serious Problems
CWE-911	Improper Update of Reference Count	5.19	Potential Problems