

CWE for C++ Rule Enforcement

Perforce QAC for C++ 2026.1

CWE enforcement is measured against defined lists of weaknesses which do not all apply to every language.

The CWEs listed are from CWE 4.19.1

2025 CWE Top 25 Most Dangerous Software Weaknesses

Rank	Rule	Rule Description	Enforced
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	No
[2]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Yes
[3]	CWE-352	Cross-Site Request Forgery (CSRF)	No
[4]	CWE-862	Missing Authorization	No
[5]	CWE-787	Out-of-bounds Write	Yes
[6]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	No
[7]	CWE-416	Use After Free	Yes
[8]	CWE-125	Out-of-bounds Read	Yes
[9]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Yes
[10]	CWE-94	Improper Control of Generation of Code ('Code Injection')	No
[11]	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Yes
[12]	CWE-434	Unrestricted Upload of File with Dangerous Type	No
[13]	CWE-476	NULL Pointer Dereference	Yes
[14]	CWE-121	Stack-based Buffer Overflow	Yes
[15]	CWE-502	Deserialization of Untrusted Data	No
[16]	CWE-122	Heap-based Buffer Overflow	Yes
[17]	CWE-863	CWE-863: Incorrect Authorization	No

Rank	Rule	Rule Description	Enforced
[18]	CWE-20	Improper Input Validation	Yes
[19]	CWE-284	Improper Access Control	No
[20]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	No
[21]	CWE-306	Missing Authentication for Critical Function	No
[22]	CWE-918	Server-Side Request Forgery (SSRF)	No
[23]	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	No
[24]	CWE-639	Authorization Bypass Through User-Controlled Key	No
[25]	CWE-770	Allocation of Resources Without Limits or Throttling	No

CWE for C++ Enforcement

Rule	Rule Description	Enforced
CWE-14	Compiler Removal of Code to Clear Buffers	Yes
CWE-20	Improper Input Validation	Yes
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Yes
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Yes
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	Yes
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Yes
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')	Yes
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	Yes
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Yes
CWE-121	Stack-based Buffer Overflow	Yes
CWE-122	Heap-based Buffer Overflow	Yes
CWE-124	Buffer Underwrite ('Buffer Underflow')	Yes

Rule	Rule Description	Enforced
CWE-125	Out-of-bounds Read	Yes
CWE-126	Buffer Over-read	Yes
CWE-127	Buffer Under-read	Yes
CWE-128	Wrap-around Error	Yes
CWE-129	Improper Validation of Array Index	Yes
CWE-130	Improper Handling of Length Parameter Inconsistency	Yes
CWE-131	Incorrect Calculation of Buffer Size	Yes
CWE-170	Improper Null Termination	Yes
CWE-176	Improper Handling of Unicode Encoding	Yes
CWE-187	Partial String Comparison	Yes
CWE-188	Reliance on Data/Memory Layout	Yes
CWE-190	Integer Overflow or Wraparound	Yes
CWE-191	Integer Underflow (Wrap or Wraparound)	Yes
CWE-192	Integer Coercion Error	Yes
CWE-193	Off-by-one Error	Yes
CWE-194	Unexpected Sign Extension	Yes
CWE-195	Signed to Unsigned Conversion Error	Yes
CWE-196	Unsigned to Signed Conversion Error	Yes
CWE-197	Numeric Truncation Error	Yes
CWE-242	Use of Inherently Dangerous Function	Yes
CWE-243	Creation of chroot Jail Without Changing Working Directory	Yes
CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	Yes
CWE-248	Uncaught Exception	Yes
CWE-259	Use of Hard-coded Password	Yes
CWE-269	Improper Privilege Management	Yes

Rule	Rule Description	Enforced
CWE-321	Use of Hard-coded Cryptographic Key	Yes
CWE-324	Use of a Key Past its Expiration Date	Yes
CWE-336	Same seed in Pseudo-Random Number Generator (PRNG)	Yes
CWE-337	Predictable seed in Pseudo-Random Number Generator (PRNG)	Yes
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Yes
CWE-364	Signal Handler Race Condition	Yes
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	Yes
CWE-375	Returning a Mutable Object to an Untrusted Caller	Yes
CWE-397	Declaration of Throws for Generic Exception	Yes
CWE-401	Missing Release of Memory after Effective Lifetime	Yes
CWE-412	Unrestricted Externally Accessible Lock	Yes
CWE-413	Improper Resource Locking	Yes
CWE-415	Double Free	Yes
CWE-416	Use After Free	Yes
CWE-457	Use of Uninitialized Variable	Yes
CWE-460	Improper Cleanup on Thrown Exception	Yes
CWE-466	Return of Pointer Value Outside of Expected Range	Yes
CWE-467	Use of sizeof() on a Pointer Type	Yes
CWE-468	Incorrect Pointer Scaling	Yes
CWE-469	Use of Pointer Subtraction to Determine Size	Yes
CWE-476	NULL Pointer Dereference	Yes
CWE-478	Missing Default Case in Multiple Condition Expression	Yes
CWE-479	Signal Handler Use of a Non-reentrant Function	Yes
CWE-480	Use of Incorrect Operator	Yes

Rule	Rule Description	Enforced
CWE-481	Assigning instead of Comparing	Yes
CWE-482	Comparing instead of Assigning	Yes
CWE-483	Incorrect Block Delimitation	Yes
CWE-484	Omitted Break Statement in Switch	Yes
CWE-489	Active Debug Code	Yes
CWE-493	Critical Public Variable Without Final Modifier	Yes
CWE-495	Private Data Structure Returned From A Public Method	Yes
CWE-500	Public Static Field Not Marked Final	Yes
CWE-543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	Yes
CWE-558	Use of getlogin() in Multithreaded Application	Yes
CWE-562	Return of Stack Variable Address	Yes
CWE-587	Assignment of a Fixed Address to a Pointer	Yes
CWE-606	Unchecked Input for Loop Condition	Yes
CWE-676	Use of Potentially Dangerous Function	Yes
CWE-690	Unchecked Return Value to NULL Pointer Dereference	Yes
CWE-704	Incorrect Type Conversion or Cast	Yes
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code	Yes
CWE-762	Mismatched Memory Management Routines	Yes
CWE-766	Critical Data Element Declared Public	Yes
CWE-767	Access to Critical Private Variable via Public Method	Yes
CWE-781	Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code	Yes
CWE-782	Exposed IOCTL with Insufficient Access Control	Yes
CWE-783	Operator Precedence Logic Error	Yes
CWE-785	Use of Path Manipulation Function without Maximum-sized Buffer	Yes

Rule	Rule Description	Enforced
CWE-787	Out-of-bounds Write	Yes
CWE-798	Use of Hard-coded Credentials	Yes
CWE-805	Buffer Access with Incorrect Length Value	Yes
CWE-806	Buffer Access Using Size of Source Buffer	Yes
CWE-839	Numeric Range Comparison Without Minimum Check	Yes
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')	Yes
CWE-910	Use of Expired File Descriptor	Yes
CWE-911	Improper Update of Reference Count	Yes

2006–2026, The MITRE Corporation.