Axivion - Technical Factsheet CWE Rules (Common Weakness Enumeration)

Version 7.12.0 upwards

Contents

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

1. C/C++

1. Common Weakness Enumeration

CWE-Rule	Severity	Description
20	High	Improper Input Validation. [Improper-Neutralization, Top25-2024-12]
22	High	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'). [File-Handling-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-5]
23		Relative Path Traversal. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
36		Absolute Path Traversal. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
77	High	Improper Neutralization of Special Elements used in a Command ('Command Injection'). [Improper-Neutralization, Top25-2024-13]
78	High	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'). [Data-Neutralization-Issues, Improper-Neutralization, Top25-2024-7]
79	High	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). [Data-Neutralization-Issues, Improper-Neutralization, Top25-2024-1]
89	High	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). [Data-Neutralization-Issues, Improper-Neutralization, Top25-2024-3]
94	Medium	Improper Control of Generation of Code ('Code Injection'). [Data-Neutralization-Issues, Improper-Neutralization, Top25-2024-11]
119	High	Improper Restriction of Operations within the Bounds of a Memory Buffer. [Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-20]
120	High	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'). [Memory-Buffer-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
121	High	Stack-based Buffer Overflow. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

123	High	Write-what-where Condition. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
124	Medium	Buffer Underwrite ('Buffer Underflow'). [Memory-Buffer-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
125		Out-of-bounds Read. [Memory-Buffer-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-6]
126		Buffer Over-read. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
127		Buffer Under-read. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
131	High	Incorrect Calculation of Buffer Size. [Memory-Buffer-Errors, Incorrect-Calculation]
134	High	Use of Externally-Controlled Format String. [String-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
135		Incorrect Calculation of Multi-Byte String Length. [String-Errors, Incorrect-Calculation]
190	Medium	Integer Overflow or Wraparound. [Numeric-Errors, Incorrect-Calculation, Top25-2024-23]
191		Integer Underflow (Wrap or Wraparound). [Numeric-Errors, Incorrect-Calculation]
192	Medium	Integer Coercion Error. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
194	High	Unexpected Sign Extension. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
195		Signed to Unsigned Conversion Error. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
197	Low	Numeric Truncation Error. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
200	High	Exposure of Sensitive Information to an Unauthorized Actor. [Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-17]
242	High	Use of Inherently Dangerous Function. [Api-Function-Errors, Improper-Adherence-To-Coding-Standards]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

243	High	Creation of chroot Jail Without Changing Working Directory. [Privilege-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
244		Improper Clearing of Heap Memory Before Release ('Heap Inspection'). [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
248		Uncaught Exception. [Error-Conditions, Insufficient-Control-Flow-Management]
252	Low	Unchecked Return Value. [Error-Conditions, Improper-Check-Or-Handling-Of-Exceptional-Conditions]
253	Low	Incorrect Check of Function Return Value. [Error-Conditions, Improper-Adherence-To-Coding-Standards]
259	High	Use of Hard-coded Password. [Improper-Access-Control, Improper-Adherence-To-Coding-Standards, Protection-Mechanism-Failure]
269	Medium	Improper Privilege Management. [Improper-Access-Control, Top25-2024-15]
271	High	Privilege Dropping / Lowering Errors. [Improper-Access-Control]
272		Least Privilege Violation. [Privilege-Issues, Improper-Access-Control]
273	Medium	Improper Check for Dropped Privileges. [Privilege-Issues, Improper-Check-Or-Handling-Of-Exceptional-Conditions]
287	High	Improper Authentication. [Improper-Access-Control, Top25-2024-14]
335		Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG). [Cryptographic-Issues, Random-Number-Issues, Protection-Mechanism-Failure]
336		Same Seed in Pseudo-Random Number Generator (PRNG). [Protection-Mechanism-Failure]
337		Predictable Seed in Pseudo-Random Number Generator (PRNG). [Protection-Mechanism-Failure]
338	Medium	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG). [Cryptographic-Issues, Random-Number-Issues, Protection-Mechanism-Failure]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

362	Medium	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'). [Insufficient-Control-Flow-Management]
369	Medium	Divide By Zero. [Numeric-Errors, Incorrect-Calculation]
378	High	Creation of Temporary File With Insecure Permissions. [File-Handling-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
379	Low	Creation of Temporary File in Directory with Insecure Permissions. [File-Handling-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
396		Declaration of Catch for Generic Exception. [Error-Conditions, Insufficient-Control-Flow-Management]
397		Declaration of Throws for Generic Exception. [Error-Conditions, Insufficient-Control-Flow-Management]
400	High	Uncontrolled Resource Consumption. [Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-24]
401	Medium	Missing Release of Memory after Effective Lifetime. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
404	Medium	Improper Resource Shutdown or Release. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
413		Improper Resource Locking. [Resource-Locking-Problems, Improper-Control-Of-A-Resource-Through-Its-Lifetime, Insufficient-Control-Flow-Management]
415	High	Double Free. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
416	High	Use After Free. [Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-8]
426	High	Untrusted Search Path. [File-Handling-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
457	High	Use of Uninitialized Variable. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
464	High	Addition of Data Structure Sentinel. [Data-Neutralization-Issues, Improper-Neutralization]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

467	High	Use of sizeof() on a Pointer Type. [Incorrect-Calculation]
468	Medium	Incorrect Pointer Scaling. [Pointer-Issues, Incorrect-Calculation]
469	Medium	Use of Pointer Subtraction to Determine Size. [Pointer-Issues, Incorrect-Calculation]
476	Medium	NULL Pointer Dereference. [Pointer-Issues, Improper-Adherence-To-Coding-Standards, Top25-2024-21]
477		Use of Obsolete Function. [Api-Function-Errors, Improper-Adherence-To-Coding-Standards]
478		Missing Default Case in Multiple Condition Expression. [Bad-Coding-Practices, Incorrect-Comparison]
480	Low	Use of Incorrect Operator. [Behavioral-Problems, Expression-Issues, String-Errors, Insufficient-Control-Flow-Management]
481	Low	Assigning instead of Comparing. [Insufficient-Control-Flow-Management]
482	Low	Comparing instead of Assigning. [Insufficient-Control-Flow-Management]
483	Low	Incorrect Block Delimitation. [Behavioral-Problems, Insufficient-Control-Flow-Management]
484	Medium	Omitted Break Statement in Switch. [Behavioral-Problems, Improper-Adherence-To-Coding-Standards]
489		Active Debug Code. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
500	High	Public Static Field Not Marked Final. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
502	Medium	Deserialization of Untrusted Data. [Resource-Management-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-16]
547		Use of Hard-coded, Security-relevant Constants. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
558		Use of getlogin() in Multithreaded Application. [Improper-Control-Of-A-Resource-Through-Its-Lifetime, Insufficient-Control-Flow-Management]
561		Dead Code. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

562		Return of Stack Variable Address. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
563		Assignment to Variable without Use. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
587		Assignment of a Fixed Address to a Pointer. [Pointer-Issues, Improper-Adherence-To-Coding-Standards]
588		Attempt to Access Child of a Non-structure Pointer. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
590		Free of Memory not on the Heap. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
595		Comparison of Object References Instead of Object Contents. [Incorrect-Comparison]
606		Unchecked Input for Loop Condition. [Data-Validation-Issues, Improper-Neutralization]
617		Reachable Assertion. [Error-Conditions, Insufficient-Control-Flow-Management]
665	Medium	Improper Initialization. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
672		Operation on a Resource after Expiration or Release. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
674		Uncontrolled Recursion. [Insufficient-Control-Flow-Management]
675		Multiple Operations on Resource in Single-Operation Context. [Improper-Adherence-To-Coding-Standards]
676	High	Use of Potentially Dangerous Function. [Api-Function-Errors, Improper-Adherence-To-Coding-Standards]
680		Integer Overflow to Buffer Overflow. [Incorrect-Calculation]
683		Function Call With Incorrect Order of Arguments. [Improper-Adherence-To-Coding-Standards]
685		Function Call With Incorrect Number of Arguments. [Improper-Adherence-To-Coding-Standards]
686		Function Call With Incorrect Argument Type. [Improper-Adherence-To-Coding-Standards]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

690		Unchecked Return Value to NULL Pointer Dereference. [Improper-Check-Or-Handling-Of-Exceptional-Conditions]
761		Free of Pointer not at Start of Buffer. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
762	Low	Mismatched Memory Management Routines. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
763		Release of Invalid Pointer or Reference. [Pointer-Issues, Resource-Management-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
766		Critical Data Element Declared Public. [Permission-Issues, Improper-Access-Control, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
767		Access to Critical Private Variable via Public Method. [Permission-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
772	High	Missing Release of Resource after Effective Lifetime. [Resource-Management-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
773		Missing Reference to Active File Descriptor or Handle. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
775		Missing Release of File Descriptor or Handle after Effective Lifetime. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
783	Low	Operator Precedence Logic Error. [Behavioral-Problems, Expression-Issues, Insufficient-Control-Flow-Management]
787	High	Out-of-bounds Write. [Memory-Buffer-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime, Top25-2024-2]
789		Memory Allocation with Excessive Size Value. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
798	High	Use of Hard-coded Credentials. [Credentials-Management-Errors, Key-Management-Errors, Improper-Access-Control, Top25-2024-22]
806		Buffer Access Using Size of Source Buffer. [Improper-Control-Of-A-Resource-Through-Its-Lifetime]
824		Access of Uninitialized Pointer. [Pointer-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

825		Expired Pointer Dereference. [Pointer-Issues, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
828		Signal Handler with Functionality that is not Asynchronous-Safe. [Insufficient-Control-Flow-Management]
831		Signal Handler Function Associated with Multiple Signals. [Insufficient-Control-Flow-Management]
839		Numeric Range Comparison Without Minimum Check. [Numeric-Errors, Incorrect-Comparison]
843		Access of Resource Using Incompatible Type ('Type Confusion'). [Type-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
910	Medium	Use of Expired File Descriptor. [Resource-Management-Errors, Improper-Control-Of-A-Resource-Through-Its-Lifetime]
1043		Data Element Aggregating an Excessively Large Number of Non-Primitive Elements. [Bad-Coding-Practices, Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1055		Multiple Inheritance from Concrete Classes. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1056		Invocable Control Element with Variadic Parameters. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1064		Invocable Control Element with Signature Containing an Excessive Number of Parameters. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1069		Empty Exception Block. [Improper-Adherence-To-Coding-Standards]
1071		Empty Code Block. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
1074		Class with Excessively Deep Inheritance. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1075		Unconditional Control Flow Transfer outside of Switch Block. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1077		Floating Point Comparison with Incorrect Operator. [Incorrect-Comparison]
1079		Parent Class without Virtual Destructor Method. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

1080	Source Code File with Excessive Number of Lines of Code. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1082	Class Instance Self Destruction Control Element. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
1086	Class with Excessive Number of Child Classes. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1087	Class with Virtual Method without a Virtual Destructor. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
1119	Excessive Use of Unconditional Branching. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1121	Excessive McCabe Cyclomatic Complexity. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1124	Excessively Deep Nesting. [Complexity-Issues, Improper-Adherence-To-Coding-Standards]
1126	Declaration of Variable with Unnecessarily Wide Scope. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
1127	Compilation with Insufficient Warnings or Errors. [Bad-Coding-Practices, Improper-Adherence-To-Coding-Standards]
1390	Weak Authentication. [Improper-Access-Control]
1391	Use of Weak Credentials. [Improper-Access-Control]

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

2. C#

1. Common Weakness Enumeration

C#-CWE-Rule	Severity	Description
20	Adv	Improper Input Validation (CWE-20): application fails to validate or sanitize input, allowing unexpected values.
22	Adv	The product uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.
77	Adv	The product constructs commands or command-like strings using externally-influenced input from an upstream component, but it does not properly neutralize or validate special elements that could change the meaning of the command when sent to a downstream component (leading to command injection or unintended command modification).
78	Adv	The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.
79	Adv	The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
89	Adv	The product constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream database.
94	Adv	Code Injection / Improper Control of Generation of Code (CWE-94): executing or compiling untrusted input as code or expressions.
269	Adv	The application performs improper privilege management, which can allow an attacker to escalate privileges or bypass access controls.
276	Adv	Incorrect Default Permissions (CWE-276): files or directories created with insecure default ACLs.
287	Adv	The application performs improper authentication, which can allow an attacker to bypass authentication mechanisms.

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868

306	Adv	Missing authentication for critical functions (CWE-306).
352	Adv	Public controller methods that change state (POST/PUT/DELETE) must enforce CSRF validation.
362	Adv	Race condition: unsynchronized access to shared resources can lead to incorrect behavior or security issues.
434	Adv	The web application allows unrestricted upload of files with dangerous types that can be automatically processed within the web server's environment.
502	Adv	Deserialization of untrusted data may lead to remote code execution or arbitrary object instantiation (CWE-502).
798	Adv	The product contains hard-coded credentials, such as passwords, API keys, or tokens, which may allow an attacker to gain unauthorized access if the source code is exposed.
862	Adv	The product does not perform an authorization check when an actor attempts to access a resource or perform an action.
863	Adv	Incorrect Authorization (CWE-863): sensitive actions performed without verifying user authorization.
918	Adv	Server-Side Request Forgery (SSRF): application issues HTTP requests to attacker-controlled URLs.

The Qt Company GmbH
Erich-Thilo-Str. 10
12489 Berlin
Deutschland

Tel. +49 30 40365640
info@qt.io
https://www.qt.io/

Geschäftsführung:
Mika Pälsi
Juha Varelius
Juha Puputti

Amtsgericht Charlottenburg (Berlin):
HRB 144331 B
USt-IdNr. DE286306868