RESORT Coverage for CWE: C

RESORT Code Analysis Version 2016 and CWE 2.9

CWE ID	RESORT Code Checker
14	Base Compiler Removal of Code to Clear Buffers
22	Path Traversal
23	Relative Path Traversal
36	Absolute Path Traversal
78	OS Command Injection
89	SQL Injection
90	LDAP Injection
99	Resource Injection
114	Process Control
119	Improper Restriction of Operations within the Bounds of a Memory Buffer
120	Classic Buffer Overflow
121	Stack-based Buffer Overflow
122	Heap-based Buffer Overflow
123	Write-what-where Condition
124	Buffer Underflow
126	Buffer Over-read
127	Buffer Under-read
129	Improper Validation of Array Index
131	Incorrect Calculation of Buffer Size
134	Uncontrolled Format String
190	Integer Overflow or Wraparound
191	Integer Underflow (Wrap or Wraparound)
194	Unexpected Sign Extension
195	Signed to Unsigned Conversion Error
196	Unsigned to Signed Conversion Error
197	Numeric Truncation Error
209	Information Exposure Through an Error Message
222	Truncation of Security-relevant Information
223	Omission of Security-relevant Information
226	Sensitive Information Uncleared Before Release
242	Use of Inherently Dangerous Function
244	Heap Inspection
247	DEPRECATED (Duplicate): Reliance on DNS Lookups in a Security Decision
252	Unchecked Return Value
253	Incorrect Check of Function Return Value
256	Plaintext Storage of a Password
259	Use of Hard-coded Password
272	Least Privilege Violation
273	Improper Check for Dropped Privileges

284	Improper Access Control
319	Cleartext Transmission of Sensitive Information
321	Use of Hard-coded Cryptographic Key
325	Missing Required Cryptographic Step
327	Use of a Broken or Risky Cryptographic Algorithm
328	Reversible One-Way Hash
338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
364	Signal Handler Race Condition
366	Race Condition within a Thread
367	Time-of-check Time-of-use (TOCTOU) Race Condition
369	Divide By Zero
377	Insecure Temporary File
390	Detection of Error Condition Without Action
391	Unchecked Error Condition
398	Indicator of Poor Code Quality
400	Resource Exhaustion
401	Memory Leak
404	Improper Resource Shutdown or Release
415	Double Free
416	Use After Free
457	Use of Uninitialized Variable
467	Use of sizeof() on a Pointer Type
468	Incorrect Pointer Scaling
469	Use of Pointer Subtraction to Determine Size
476	NULL Pointer Dereference
478	Missing Default Case in Switch Statement
479	Signal Handler Use of a Non-reentrant Function
480	Use of Incorrect Operator
481	Assigning instead of Comparing
482	Comparing instead of Assigning
483	Incorrect Block Delimitation
484	Omitted Break Statement in Switch
495	Variant Private Array-Typed Field Returned From A Public Method
496	Variant Public Data Assigned to Private Array-Typed Field
561	Dead Code
562	Return of Stack Variable Address
570	Expression is Always False
571	Expression is Always True
587	Assignment of a Fixed Address to a Pointer
590	Free of Memory not on the Heap
601	Open Redirect
615	Information Exposure Through Comments
665	Improper Initialization

674	Uncontrolled Recursion
675	Duplicate Operations on Resource
676	Use of Potentially Dangerous Function
680	Integer Overflow to Buffer Overflow
685	Function Call With Incorrect Number of Arguments
688	Function Call With Incorrect Variable or Reference as Argument
690	Unchecked Return Value to NULL Pointer Dereference
759	Use of a One-Way Hash without a Salt
762	Mismatched Memory Management Routines
789	Uncontrolled Memory Allocation
835	Infinite Loop
843	Type Confusion

Soft4Soft Co., Ltd.

501 ETRI CTC Center, 218, Gajeong-ro, Yuseong-gu, Daejeon, 305-700, KOREA

TEL. +82-2-553-9464, www.soft4soft.com, Email: info@soft4soft.com