

Part 3 – Secure Coding Project (PV193) (static checker)

Code Project Name: Sequence Chart Studio (scstudio)

Description : Scstudio is a user-friendly drawing and verification tool for Message Sequence Charts (MSC, HMSC) and UML Sequence Diagrams. This is integrated with Microsoft Visio. For compilation is needed CMake and C/C++ compiler

Details of codes: 70K lines code (1276 files)

URL: <http://sourceforge.net/projects/scstudio/?source>

Checked with Tool: Cppcheck/ Valgrind

I. Cppcheck: In this source code, same type of errors was identified in various file and function. The summary of the errors is described as under:-

<u>S.No</u>	<u>Error category</u>	<u>Type of Error</u>	<u>Remarks</u>
1.	Information	(a) The code 'class SCZ120_EXPORT Z120 :' is not handled. You can use -I or --include to add handling of this code. (b) The code 'class SCMSC_EXPORT Checker:' is not handled. You can use -I or --include to add handling of this code. (c) The configuration '_MSC_VER' was not checked because its code equals another one.	Class is not used
2.	Performance	(a) Variable 'm_sender' is assigned in constructor body. Consider performing initialization in initialization list. (b) Prefer prefix ++/-- operators for non-primitive types. (c) Possible inefficient checking (d) Reassigned a value before the old one has been used	Check input/output operations
3.	Style	(a) Variable 'path' is allocated memory that is never used. (b) Unused variable: msc_b (c) The scope of the variable 'result' can be reduced. (d) Variable 'message' hides enumerator with same name (e) Checking if unsigned variable 'proto' is less than zero	Check input/output operations

		(f) C-style pointer casting (g) The exception is caught by value. It could be caught as a (const) reference which is usually recommended in C++. (h) Statements following return, break, continue, goto or throw will never be executed.	
4.	Portability	The extra qualification 'CShapeUtils::' is unnecessary and is considered an error by many compilers	Incorrect use of functions from Standard Template Library
5.	Error	(i) Possible null pointer dereference: eti (ii) Uninitialized variable: c2_ptr_out (iii) Memory leak: s (iv) Resource leak: content_types_file (vi) Invalid number of character (l) when these macros are defined: ".	Null pointer dereferencing Due to lost scope without de-allocation Due to forgetting to close a file handler

II. Valgrind report:

```

==17191== HEAP SUMMARY:
==17191==   in use at exit: 6,869 bytes in 72 blocks
==17191== total heap usage: 772 allocs, 700 frees, 349,507 bytes allocated
==17191==
==17191== 6,869 (224 direct, 6,645 indirect) bytes in 1 blocks are definitely lost in loss record 51 of
51
==17191==   at 0x4C2A0D7: operator new(unsigned long) (in
/usr/lib64/valgrind/vgpreload_memcheck-amd64-linux.so)
==17191==   by 0x4F18774: new_hmsc_fun (in /home/ado/scstudio-
code/src/data/Z120/libscZ120.so)
==17191==   by 0x4F84186: hmsc (in /home/ado/scstudio-code/src/data/Z120/libscZ120.so)
==17191==   by 0x4F50820: message_sequence_chart (in /home/ado/scstudio-
code/src/data/Z120/libscZ120.so)
==17191==   by 0x4F4D240: textual_msc_file (in /home/ado/scstudio-
code/src/data/Z120/libscZ120.so)
==17191==   by 0x4F0F340: Z120::load_msc(std::string const&, std::string const&) (in
/home/ado/scstudio-code/src/data/Z120/libscZ120.so)
==17191==   by 0x4052B1: main (in /home/ado/scstudio-code/tests/z120_test/z120_test)
==17191==
==17191== LEAK SUMMARY:
==17191==   definitely lost: 224 bytes in 1 blocks
==17191==   indirectly lost: 6,645 bytes in 71 blocks
==17191==   possibly lost: 0 bytes in 0 blocks
==17191==   still reachable: 0 bytes in 0 blocks
==17191==     suppressed: 0 bytes in 0 blocks
==17191==

```