

Static Analysis of LibVNCServer-0.9.9 using Cppcheck

Error			
File	Line No.	Summary	Remark
\examples\pnmshow.c	69	Resource leak: in	FILE handler not released. return before fclose(in)
\examples\pnmshow24.c	64	Resource leak: in	FILE handler not released. return before fclose(in)
\libvncserver\font.c	177	Resource leak: f	FILE handler not released. return before fclose(f)
\libvncserver\rfbserver.c	1585	Common realloc mistake: 'buffer' nulled but not freed upon failure	buffer needs to be released when realloc fails
\libvncserver\tight.c	352,633, 642, 1582	Common realloc mistake: 'tightBeforeBuf', 'tightBeforeBuf', 'tightAfterBuf', 'tightAfterBuf' nulled but not freed upon failure	False Positive : 'tightBeforeBuf', 'tightBeforeBuf', 'tightAfterBuf', 'tightAfterBuf' freed in function rfbTightCleanup
\libvncserver\zlib.c	106,146	Common realloc mistake: 'zlibBeforeBuf', 'zlibAfterBuf' nulled but not freed upon failure	False Positive : 'zlibBeforeBuf', 'zlibAfterBuf' freed in function rfbZlibCleanup
\libvncserver\cargs.c	126	Memory leak: passwd	Memory not released
\vncterm\LinuxVNC.c	190	Memory leak: buffer	buffer memory not released
\examples\example.c	276	Memory leak: c->richSource	False positive: Memory released at function 'void rfbFreeCursor(rfbCursorPtr cursor)' line no 350 in file libvncserver\cursor.c
\client_examples\scrap.c	263	Uninitialized variable: retval	Since there is no explicit initialization of 'retval' and if preprocessors and conditions are used for assigning variable value.
\common\turbojpeg.c	465,466,466,468, 8,645,646,648	Possible null pointer dereference: this - otherwise it is redundant to check it against null.	Pointer 'this' is already dereferenced before checking if it for being NULL
\test\cursortest.c	239	Possible null pointer dereference: c - otherwise it is redundant to check it against null.	Pointer 'c' is already dereferenced before checking if it NULL
\common\lzoconf.h	66	check your compiler installation	Due to error preprocessor used as part of error handling
\common\lzoconf.h	139	lzo_uint	Due to error preprocessor used as part of error handling
\common\lzoconf.h	158	lzo_uint32	Due to error preprocessor used as part of error handling
\common\lzoconf.h	63	#error "invalid CHAR_BIT"	Due to error preprocessor used as part of error handling
\common\lzodefs.h	1059	LZO_SIZEOF_SHORT	Due to error preprocessor used as part of error handling

Static Analysis of LibVNCServer-0.9.9 using Cppcheck

\\common\\lzdefs.h	1080	LZO_SIZEOF_INT	Due to error preprocessor used as part of error handling
\\common\\lzdefs.h	1097	LZO_SIZEOF_LONG	Due to error preprocessor used as part of error handling
\\libvncclient\\hextile.c	94	Invalid BPP	Due to error preprocessor used as part of error handling
\\libvncclient\\hextile.c	94	#error "Invalid BPP"	Due to error preprocessor used as part of error handling
\\libvncserver\\tableinitcmtemplate.c	37	It is included as part of translate.c	Due to error preprocessor used as part of error handling
\\libvncserver\\tableinitcmtemplate.c	36	#error "This file shouldn't be compiled."	Due to error preprocessor used as part of error handling
\\libvncserver\\tableinitctemplate.c	39	It is included as part of translate.c	Due to error preprocessor used as part of error handling
\\libvncserver\\tableinitctemplate.c	38	#error "This file shouldn't be compiled."	Due to error preprocessor used as part of error handling

Warning

File	Line No.	Summary	Remark
\\libvncserver\\httpd.c	374	scanf without field width limits can crash with huge input data.	Warning has been addressed by putting limit: if (strlen(buf) > maxFnameLen)
\\LibVNCServer-0.9.9\\test\\bmp.c	121	scanf without field width limits can crash with huge input data.	Warning has been addressed by putting limit : if(!fgets(temps, 255, fs))

Summary

Errors-35	Warnings-02	Style Warnings-70
Resource leak-03 Common realloc mistake: 07 Memory Leak -03 Uninitialized variable-01 Possible null pointer dereference-08 Error preprocessor-13	scanf without field width limits can crash with huge input data.-02	Variable is assigned a value that is never used-08 Unused variable-08 The scope of the variable can be reduced-49 Checking if unsigned variable 'jpegSize' is less than zero-02 Found duplicate branches for if and else-02 Clarify calculation precedence for + and ? -01