



NYSBOE ES&S and Dominion Source Code Review Validation for NYSTEC

August 31, 2012

Contact:

Program Management: Dr. Vincent DiLosa

Contracts: Danielle Mahoney/John Purdon

SRA International

8830 Stanford Blvd, Suite 205

Columbia, Maryland 21045

Main Office: 410.715.9399

Fax: 410.715.9397

Table of Contents

- 1 Executive Summary 3
- 2 References 3
- 3 Appendix 3
 - 3.1 General Review Comments 4
 - 3.2 Dominion 5
 - 3.2.1 BMDVideo v.4.9.6 5
 - 3.2.2 EMS v.4.9.17 5
 - 3.2.3 ICC v.4.9.13 9
 - 3.2.4 ICP v.4.9.9 10
 - 3.3 ESS 14
 - 3.3.1 Automark v.1.8.1.1a 14
 - 3.3.2 EMS 14
 - 3.3.3 DS200 v.2.7.0.1i 17
 - 3.3.4 DS850 v.2.4.0.1b 18

1 Executive Summary

At the request of NYSTEC, SRA International, Inc. reviewed the electronic voting system source code security analysis conducted by Wyle Labs and verified by SLI technical reviewers. We reviewed the documents and source code listed in References to attempt to determine if the results were reasonable and complete. The methodology used in the code review of the ES&S and Dominion software appears to be sound. Using a combination of automated tools along with manual code review is a good method for identifying possible security issues in the code. Based on our review we assert that the source code security analysis performed by the vendors was reasonably complete. Our detailed comments are presented in the Appendix.

2 References

ESS:

NYSBOE ESS Upgrade Source Code Review Report (CC) v1.0_Final.pdf
NYSBOE ESS Upgrade Source Code Review Report (Non CC) v1.0_F.pdf

ESS_Consolidated_SCRDRF_2009_to_2012_Final.xlsx –
AutoMARK VAT v.1.8.1.1a
EMS
DS200 v. 2.7.0.1i
DS850 v. 2.4.0.1b

Dominion:

NYSBOE DVS Upgrade (BMD) Source Code Review Report v1.0.pdf
NYSBOE DVS Upgrade (EMS_ICP) Source Code Review Report v1.0.pdf

DVS_Consolidated_SCRDRF_2009_to_2012_ALL_ITEMS.xls –
BMDVideo v.4.9.6
EMS v.4.9.17
ICP 4.9.9
ICP v.4.9.13

And associated Dominion and ESS code as contained on CDs received by SRA in August 2012.

3 Appendix

SRA International analyzed the source code review results of the ES&S and Dominion code for NYSTEC to ascertain whether due diligence was performed by the vendors. The focus of our evaluation was on items that could have security and reliability implications to the system. We did not review style and commenting issues. Although we found the review appropriate, no

software code is faultless and we offer some comments on improvements for future versions. This Appendix details our technical findings.

3.1 General Review Comments

A number of observations remain from our previous analysis. There are many instances of code that is commented out of the source code. We recommend removing 'commented out' code before release.

Enforce singleton principle throughout codebase. None of the singletons used private constructors, allowing them to be instantiated multiple times. And multiple "get" instance functions did not check if the instance was instantiated or not before trying to return it.

Java garbage collection cannot be forced to run. Therefore by not closing handles, etc, it causes the java heap to fill. Relying on the native garbage collection to close opened handles, etc is not a good programming practice.

Software revisions not matching and references to future revisions make the code review verification more difficult, take more time and make it less effective. For example, the version of ICC in the DVS spreadsheet is v.4.9.13. The code we received is v.4.9.14. This was the case for many different packages we reviewed.

Due to limited knowledge of the build and run environments, some of the conclusions reached cannot necessarily be definitive. Is any of the code used in a multithreaded environment? There are many global variables and some static buffers used throughout the code without any locking mechanisms. This could lead to possible bugs, security problems, race conditions and/or deadlock problems. We recommend minimizing or eliminating the use of global variables and static buffers unless they are constants.

A main concern after performing the review continues to be the maintainability of the code. There are many hardcoded values in the code which make the code susceptible to errors if the code is modified and rebuilt. Some of these are used in loops and buffer declarations so they could cause security issues if the developer makes a change in one part of the code without realizing it impacts another part of the code base. Using constants can eliminate these issues. When the value is changed in one place all of the code references automatically use the updated value.

We did not find many major problems in the code but there were a few instances of improper data handling. The issues that we feel are most important to fix start with ***. Copying data into a buffer allocated in a program should always be limited to the size of the destination buffer. Relying on the data being formatted in an expected manner is a bad security practice and can lead to many security problems. Several of these types of problems were found in our code sampling review. One instance was found involved reading data from an usb device without bounds checking. This issue should be remedied in future releases as it has the potential to create a serious security issue.

Certain types of security problems not listed as part of the methodology used in the review are still worth mentioning. For example, memory usage problems are best found by run time analysis programs and are usually not detected by automated code review tools. Logic bugs and hard to find memory bugs such as using memory after it has been freed can lead to security problems. We note that these types of bugs were not included in the list of criteria in the SLI review report. We recommend that this type of analysis be part of future reviews.

3.2 *Dominion*

The following section details the result of our review of the discrepancy reports found in the DVS_Consolidated_SCRDRF_2009_to_2012_ALL_ITEMS.xls spreadsheet. The results from each tab from the spreadsheet are contained in a separate section. The numbering scheme used for all sections is the row number of the spreadsheet.

3.2.1 BMDVideo v.4.9.6

Verified with BMDvideo-20120613-4.9.6-src code

9-113 Minor non-security related style/comment issues.
114 sprintf was changed to snprintf with proper size arguments.
115-434 Minor non-security related style/comment issues.

3.2.2 EMS v.4.9.17

Verified with EMSSourceCode_package_4.9.17

9-227 Minor non-security related style/comment issues.
228 A default case statement was added.
229-549 Minor non-security related style/comment issues.
550 Can't find corresponding code.
551-772 Minor non-security related style/comment issues.
773 Changed to explicit comparison.
774 Minor style issue.
775-776 Changed to explicit comparison.
777-1117 Minor non-security related style/comment issues.
1118 Can't find corresponding code.
1119-1139 Minor non-security related style/comment issues.
1140 Can't find SetInput call or corresponding code.
1141-1142 Minor non-security related style/comment issues.
1143 Changed to explicit comparison.

1144-1257 Minor non-security related style/comment issues.
1258 Changed to explicit comparison.
1259-1718 Minor non-security related style/comment issues.
1719 Changed to explicit comparison.
1720-2111 Minor non-security related style/comment issues.
2112-2113 Variables are now initialized.
2114-2115 Minor non-security related style/comment issues.
2116-2117 Variables are now initialized.
***2118 contestPageLocation still not initialized.
2119 Minor non-security related comment issue.
2120 All short variables are now initialized.
2121-2135 Minor non-security related style/comment issues.
2136 All short and ushort variables are now initialized.
2137-2138 Minor non-security related style/comment issues.
***2139 Variables still not initialized.
2140-2454 Minor non-security related style/comment issues.
2455 Variables are initialized.
2456 Class variables no longer appear in the class.
2457 Class variables file path and tabulator no longer appear in the class.
2458 Variables are now initialized.
2459-2606 Minor non-security related style/comment issues.
2607 There are no case statements in this file.
2608-2675 Minor non-security related style/comment issues.
2676-2682 File does not exist in code provided.
2683-2739 Minor non-security related style/comment issues.
2740 Function CalculateEllipseParams and variables ovalCenterX,Y do not appear in this file.
2741-2878 Minor non-security related style/comment issues.
2879 Variables are initialized.
2880-2935 Minor non-security related style/comment issues.
2936 Throw is now commented out.
2937-2973 Minor non-security related style/comment issues.
2974-2975 File was deleted.
2976 Minor non-security related comment issue.
2977 File was deleted.
2978-2979 Minor non-security related style/comment issues.
2980-2983 File was deleted.
2984 There is a throw outside of a catch block.
2985 Minor non-security related comment issue.
2986 Probably not a problem because data.ReadUShort() should not return something greater than short.MaxValue. The comparison could be changed to (identifier >= short.MaxValue).
2987-3196 Minor non-security related style/comment issues.
3197 Added error checking to avoid divide by zero exception.
3198-3396 Minor non-security related style/comment issues.
3397-3402 File is not in the code provided.
3403-3647 Minor non-security related style/comment issues.
3648 All switch statements have default cases.

3649-3798 Minor non-security related style/comment issues.
3799-3802 All switch statements have default cases.
3803 Minor non-security related comment issue.
3804-3807 All switch statements have default cases.
3808 Minor non-security related comment issue.
3809 All switch statements have default cases.
3810-3847 Minor non-security related style/comment issues.
***3848 The code is unchanged. If clearing the log is an issue it still exists.
3849-3850 time/date is not added.
3851-3854 Minor non-security related style/comment issues.
3855 The exception is now logged.
***3856 * is not in front of .otf as it is for other file extensions. This looks like it is still an oversight.
3857-3858 Minor non-security related style/comment issues.
3859 The exception is now logged.
3860 Minor non-security related comment issue.
3861 Comment now states that colPallete.Entries has same number of elements as ColorPlace.Pallete.
3862-3863 container appears not to be used.
3864 The call is still made with no check.
3865 There was a check added "if (rtf.Count > 0) //for first pass only"
3866-3867 Agree with description.
3868-3870 Minor non-security related style/comment issues.
3871 Debug write is still in the code.
3872-3877 Minor non-security related style/comment issues.
3878-3880 Arguments are not checked for null.
3881-3883 Minor issues.
3884 success value is now checked.
3885-3889 Minor non-security related style/comment issues.
3890 It's unclear how errorCode can be overwritten accidentally
3891 Minor issue.
3892 Agree with vendor response.
3893 Minor issue.
3894 Exception logging was added.
3895 conIndex is now incremented so it should work properly.
3896-3897 Minor issues.
3898 Default case statement was fixed.
3899 Default case statement was added.
3900-3901 Default case statements were added.
3902-3907 Minor non-security related style/comment issues.
3908 The logic has been fixed to be clearer.
3909 The switch statement has a default case.
3910 They are now logged.
***3911 Error is still not logged.
3912-3913 Agree with vendor response.
3914 Minor issue.

***3915 height is never range checked and it is used to control the loop. This is a potential problem.

3916 Parameters are not validated.

3917-3918 Parameters are not validated before use.

3919 Parameters are now initialized.

3920 args[0] not validated before use.

3921 dlg still not checked for null before reference.

3922 pd not checked for null before reference.

3923 input and result not checked. Result is referenced without validating.

3924 Minor issue.

3925 Unlikely to happen because it will be populated by BatchProcessHelper.RunProcess() if there is an error.

3926 Can't find code referenced.

3927-3929 Parameters still used extensively without checking validity.

3930 This does not seem to be an issue.

3931 File not in the code provided.

3932-3935 The parameters are just passed on. Not sure if they need validation.

3936 Return has been removed for DeleteAction case.

3937 File not in the code provided.

3938-3943 Variable validation issues.

3944 Return removed from if statement.

3945-3960 Minor or Variable validation issues.

3961 No checking for division by zero.

3962-3964 No overflow checking added. Even though it is unlikely the checking should still be added.

3965 No divide by zero checking. Even though it is unlikely the checking should still be added.

3966-3967 No overflow checking added. Even though it is unlikely the checking should still be added.

3968-3985 Minor non-security related style/comment issues.

3986-3987 Variable validation issues.

3988-3999 Minor non-security related style/comment issues.

4000 Multiple returns were removed.

4001 Added error message box.

4002 Minor non-security related style/comment issue.

4003 Comment too vague to validate.

4004 Exception message still not logged or saved.

4005-4014 Minor non-security related style/comment issue.

4015 Agree with comment.

4016 Logging not added.

4017 The merge exception is logged but no other exceptions are logged.

4018-4020 Minor non-security related style/comment issues.

4021 Logging was added.

4022 This was done to eliminate ambiguous characters as stated in the comment. It does not significantly affect the randomness of the password.

4023 No range check. Should be added.

4024 No range check. Should be added.

4025 Added range check for using data[index_].
4026 No range check. Should be added.
4027 The random number is for the volume serial number. Does this need to be FIPS compliant?
4028 Minor non-security related style/comment issue.
4029-4031 Multiple returns were removed.
4032 Default case added.
4033 Minor non-security related style/comment issue.
4034 Default case added.
4035 Minor non-security related style/comment issue.
4036 This code was removed.
4037 Code was fixed to check correct return values.
4038-4039 Minor non-security related style/comment issues.
4040 It is a confusing way of checking the function success which could be simplified. The return value problem was fixed.
4041 The return value problem was fixed.
4042 This still appears to be a problem.
4043 This was fixed with null checking added.
4044-4045 Minor non-security related style/comment issues.
4046 There are no List<String> objects in this call. Exceptions with return codes appear to be handled properly.
4047 Multiple returns removed.
4048 Call does not exist in code. Looks like a mismatch in the spreadsheet.
4049 Multiple returns removed.
4050 Default case statement added.
4051 Fixed.
4052 Default case statement added.
4053-4058 Minor non-security related style/comment issues.
4059 Added cursor assignment before the break.
4060 Logic was reworked.
4061-4062 Default case statement added.
4063 Added null checking.
4064 Call is not in the code.
4065 Default case statement added.
4066 else was deleted.
4067-4070 Minor non-security related style/comment issues.
4071 Spreadsheet columns are off by one. This code has been deleted.
4072 The user input is not sanitized here.

3.2.3 ICC v.4.9.13

Verified with ICC_4.9.14_120821 code

9 The target buffer m_label is still hardcoded to 32 bytes while BECHMARK_NAME_MAX is defined to be 200. Even if this is not included in the released code it should still be fixed.

10 Fixed
11 Default is first case (DCF_BCTYPE_3of9) not sure if this should be the default.
12-13 Fixed
14-15 Minor non-security related style issues.
16 Fixed
17 Vendor response is accurate.
18 Agree with vendor response
19-20 Minor non-security related comment issues.
21 Agree with vendor response.
22 Buffer size was increased to 1000 bytes so there is no security issue in the code as is but the code is not easily maintainable. Security issues could be reintroduced if the #defines or code are changed. We would recommend the code be reworked for better maintainability.
23 Fixed
24 Macro was replaced with code.
25-26 Fixed by checked for null pointers.
27 Fixed by replacing buffer with CString object that automatically allocates buffer space.
28 Code is commented.
29-31 Default cases were added to the switch statements.
32 NULL checks were added.
41 This is fixed by adding if else condition.
42-43 Macros were replaced.
44 Minor non-security related comment issue.
45 Most appear to be fixed but on lines 326,328,332 choice is referenced without checking to see if it is NULL first. In lines 357,358,514 con is referenced without testing for NULL. All other input pointers are tested for NULL before being dereferenced.
46 Added NULL checking.
47 Macro was replaced with code.
48 Fixed by replacing buffer with CString object that automatically allocates buffer space.
49 Fixed by replacing buffer with CString object that automatically allocates buffer space.
Global references in function comment header should be removed because they are no longer used.
50-51 The code is fixed to find the correct min and max.

3.2.4 ICP v.4.9.9

Verified with ICP_4.9.10-US_2012.Aug.16 code

9-15 Minor non-security related issues.
16-17 Problem was fixed
18-37 Minor style issues
38-42 date/time still not logged. Is this an issue?
43-48 Minor non-security related issues.
49 strcat changed to strncat with secure usage
50-60 Minor non-security related style/comment issues.
61 Changed to do while
62 The function GetAudioLanguage was removed.

63 Minor non-security related issue.

64 Exception handling was added. Error is sent to stout and not stderr.

65 tmpPassword is not longer in the code.

66 pwEntered[NUM_DIGITS_PASSWORD+1] is not initialized on lines 1187,1320.
secondPWEntered is not initialized on line 7038.

67-71 Minor non-security related issues.

72 fileName is now initialized. filesList and fhIn are still not initialized explicitly but they are initialized by later calls.

72-103 Minor non-security related style/comment issues.

104 Can't find any issues with initialization in the code. The only parameter is a NULL, so either its 0 (NULL) or its not (TRUE). No issues here. Inefficient to check before use.

105-109 Minor non-security related style/comment issues.

110 pWmarkHeight is only referenced in the ScanVoteCreateWatermark call. It is still dereferenced without checking for NULL.

111 There is no call to CDvsScanVote::ScanVoteSaveImages.

112-141 Minor non-security related style/comment issues.

142 logRC and logBackupRC are not referenced in CDvsController::ShutdownSystem()

143-149 Minor non-security related issues.

150 The strncat calls have been changed to use the remaining size of the destination buffer as the last argument which is correct.

151-168 Minor non-security related style/comment issues.

169 Variables pChoiceInstTotal and pFirstInstTotal are not longer in main.cpp.

170-203 Minor non-security related style/comment issues.

204 Can't find function printLogging or anywhere TRUE is used as an array index value.

205-209 Minor non-security related style/comment issues.

210 The sizes have been fixed to be the remaining buffer size in the destination buffer.

211-212 Minor non-security related style/comment issues.

213-214 The way the code is implemented will not cause a buffer overrun but it relies on the buttonKeys array being initialized properly. Explicit bounds checking should be added so modifications to the code can't cause buffer overrun conditions.

215-216 Minor non-security related issues.

217 Error checking was added for NULL pointer.

218 The pointer is assigned to another pointer variable and is not dereferenced.

219 Minor style issue.

***220 Size is still not checked and possibly memory is never allocated properly because it is relying on the initializer {0} which will allocate one element set to 0. This looks like a potential serious problem in the code probably a buffer overflow.

221 DVS_LOG call is made inside the while loop.

222 Minor style issue.

223 Checking for numRecords == 0 has been added.

***224-227 There is still no range checking. The values are just passed to other functions which also do not have range checking.

228-229 Minor line length issue.

***230-231 fhIn still is not null validated before use. This is a pointer and not a copy of the object, it would needs to be null checked.

232 Minor line length issue.

233 Added scanError checking to first condition.
234-239 The program logic has been changed to not overwrite error RC error conditions.
*** 240 Agree with description. Can't find the definition of DVS_APP_RELEASE. sprintf should also not be used without bounds checking.
241 Minor line length issue.
***242 Agree with description. Problem still exists in the code. If DisplayText is called with a string > (CFLOAD_LCDBUFF_SIZE + LCD_COMMAND_MAX_LENGTH -3) in length the stack buffer msg will be overflowed.
243 Minor line length issue.
244 Changed printf to LogMsg.
245 Minor line length issue.
246 Changed printf to LogMsg.
247 The response is accurate but the loop is confusing as well as a bad coding practice.
248-249 Minor non-security related style/comment issues.
250-251 Minor issue and can't locate the header file in the code provided to us.
252-320 Part of COLILO open source boot loader. The code was not provided to us as part of the review.
321-327 Minor non-security related style/comment issues.
328 Line number(s) does not match file provided to us. Not sure what comparison to which they refer.
329-333 Minor non-security related style/comment issues.
334-335 Line number(s) does not match file provided to us. Not sure what comparison to which they refer.
336-363 Minor non-security related style/comment issues.
364-366 The function calls cited do not appear in the code provided.
367-413 Minor non-security related style/comment issues.
414 Comparisons are explicit.
415 Minor non-security related style/comment issue.
416 The function calls cited do not appear in the code provided.
417-441 Minor non-security related style/comment issues.
***442 The comment is valid. This is still a minor issue.
443-445 Minor non-security related style/comment issues.
446 They are global class instances that do not need to be initialized.
447-689 Minor non-security related style/comment issues.
690 All switches have default cases.
691-715 Minor non-security related style/comment issues.
716-717 strncpy is used with sizeof destination buffer. It is currently not a problem but strncpy should use sizeof(gDeviceVersions[id].idStr) instead of sizeof(gDeviceVersions[0].idStr) in case the sizes are not the same.
718-858 Minor non-security related style/comment issues.
859 There is no destructor declared in the file.
860-922 Minor non-security related style/comment issues.
923-924 #if 0 code removed.
925-1026 Minor non-security related style/comment issues.
1027 strcat parameters were fixed to reflect the amount of buffer size available in the destination buffer.

1028-1029 Parameters are not validated but it is not an issue if parameter checking is done before the calls are made.

1030 The parameters are numbers so validation may not be necessary.

1031 The function is type VOID and no longer returns a value. There is no failure condition to log. This seems to be the intent of the developer.

1032 It is no longer implemented by division. It is now shifting which is ok with a value of zero.

1033-1142 Minor non-security related style/comment issues.

1143-1144 Range checking was added.

1145-1146 Minor non-security related style/comment issues.

1147 Checking is done in the NextRasterIndex call.

1148-1163 Minor non-security related style/comment issues.

1164-1165 There is no range or null checking for gXspotHead. This is probably not an issue because of the following. aBallotAddXspot, aBallotAddString both validate page is less than MAX_PAGE_SIDES before calling addRasterToImage, and since addRasterToImage is an internal function, as long as the external facing functions are protecting the bounds, the internal doesn't need to protect them. Good code practice yes, but does hurt efficiency in embedded systems. Also, as gXspotHead is an array of pointers, that have space malloc'd for those pointers during init of the variable, and space for the objects they point too in the call to ensureXspotEntry on line 788.

1166-1172 Minor non-security related style/comment issues.

1173 Bounds checking was added.

1174-1180 Minor non-security related style/comment issues.

1181 Boundary check added.

1182 Retrieving plane data. As long as it is checked when populated it should be ok but extra checking would not hurt. More time could be applied to verify code populating plane data.

1183-1207 Minor non-security related style/comment issues.

***1208 There is no boundary check and no way to know how much data the buffer can hold. This function should be fixed! As it is reading from the USB UART, it would be possible for a usb device (thumb drive) to overflow this buffer, and possibly lead to code execution.

1209-1247 Minor non-security related style/comment issues.

1248 There is buffer checking. It is difficult to verify it is correct because the data buffer is dynamically allocated and different constants are being used in the checks.

1249 Minor non-security related style/comment issue.

1250 This is an invalid or mismatching comment because there is no code in the header file referenced.

1251 There is buffer checking. It is difficult to verify correctness because the data buffer is dynamically allocated and different constants are being used in the checks.

1252-1282 Minor non-security related style/comment issues.

***1283 This is a classic misuse of strcat that leads to exploitable buffer overflow conditions. The source buffer size is being used as the last argument instead of the destination buffer size. This should be fixed!

1284-1686 Minor non-security related style/comment issues.

1687 The problem was fixed.

1688 Minor non-security related style/comment issue.

1689 Added NULL checking.

1690-1693 Minor non-security related style/comment issues.

1694 Fixed
1695 Added retCode checking.
1696-1746 Minor non-security related style/comment issues.
1747-1748 Calls to strncpy were fixed to use correct amount of free space in destination buffer.
1749-1753 Minor non-security related style/comment issues.
1754 The buffer is checked in the code before the strncpy.
1755-1756 strncpy size parameter has been fixed.
1757-1770 This file was deleted from the review (from Dominion File Changed Hash.xlsx)
1771-1962 Minor non-security related style/comment issues.
1963 Changed to strncpy with proper arguments.
1964 Changed to snprintf with proper arguments.
1965 The check for buffer length is done before strcpy is called. This is valid assuming gLogBuff is the size of LOGBUFF_SIZE.

3.3 ESS

The following section details the result of our review of the discrepancy reports found in the ESS_Consolidated_SCRDRF_2009_to_2012_Final.xlsx spreadsheet. The results from each tab from the spreadsheet are contained in a separate section. The numbering scheme used for all sections is the row number of the spreadsheet.

3.3.1 Automark v.1.8.1.1a

Verified with VAT_1.8.1.1a_Source

9-33 Minor non-security related style/comment issues.
34 There is no null check for m_text and it is referenced.
35-38 Minor non-security related style/comment issues.
***39 This is a flaw in the code. The second memcpy should increment the buffer by the same amount as the previous memcpy.
memcpy(tempPtr+(tempSize[currEleIDX]*sizeof(wchar_t)),buffer,len*sizeof(wchar_t));
40-60 Minor non-security related style/comment issues.
61 There is a comment in the header that the programmer must ensure the buffer is large enough to fix the version string.
62-74 Minor non-security related style/comment issues.
75-76 Default case statements were added.

3.3.2 EMS

Verified with

EssSource(CB_Evt_2.1.0.1a_Source,CB_XML_2.1.0.1a_Source,CB_XMLConv_2.1.0.1a_Source,CreateLog_1.5.0.1a_Source,electionware_4.1.0.1o_SourcePkg,

ElectionWarePaperBallot_3.1.0.1d_Source,ERM_8.6.0.2c_Source,ERMXMLConvDLL_3.1.0.1a_Source,ERMXMLDATA_2.1.0.1a_Source,EssEvt_1.5.0.1a_Source,EssEvtA_1.5.0.1a_Source,EssEvtMsg_1.5.0.1a_Source,EssXml_4.1.0.1a_Source,EvtSvc_1.5.0.1a_Source,EXITWIN_2.1.0.1a_Source,libCoNG_1.2.0.1d_Source,LogEvent_1.5.0.1a_Source,MYDLL_2.1.0.1b_Source,RegUtil_2.1.0.1a_Source,RmuCli_1.4.0.1a_Source,RmuDll_1.4.0.1a_Source,RmuSvc_1.4.0.1b_Source,RSACrypto_3.1.0.1a_Source,Shell_2.1.0.1a_Source,ShellSetup_2.1.0.1a_Source)

***9 - This does not seem correct that the database transaction is always committed even in the case of errors.

10 BufferedReader still not closed.

11 There is no check for divide by zero. It can happen if this is called before realZoom is set to a non-zero value.

12 They will close automatically when they go out of scope.

13 Function has no return value.

14 It is now added to the audit output.

15 The warning message it still not logged.

16 Default case added to the switch statement.

17-18 Minor non-security related style/comment issues.

19 Auditing added.

20 Validation may not be needed if other function can handle a zero value.

21 Auditing added.

22-120 Minor non-security related style/comment issues.

121-129 Code not provided.

130-467 Minor non-security related style/comment issues.

468 I don't see anywhere length is cast to int.

469 File not provided.

470-480 Appears to be fixed by moving to get action to assure there is only one instance.

481-482 Agree with comment.

483-485 File not provided with review.

486-487 File not provided with review. If printStackTrace is there it can expose information that can help an attacker.

488-500 Singleton is not implemented properly. The author fails to make the constructor private to enforce the Singleton property. The author uses lazy loading in the factory method "get()", which is adequate. The factory method "get()" probably should have been called "getInstance()", but that's a style issue.

501 File not provided with review.

502-504 Agree with comment.

505 No assert usage is in the code.

506 Agree with comment an external application (LogEvent.exe) is spawned with a relative path that can be a security problem.

507-521 Singleton is not implemented properly. The getInstance() method should do the instantiation of 'instance' rather than the constructor. The constructor should also be private. You would remove the block starting "if (instance == null)" from the constructor and put the following in getInstance().

522 There is still no logging of the message.

***523 It runs rmucli with a relative path that can be a security problem.

524 No assert usage is in the code.
525 toolbar is initialized.
526 mouse is no longer modified inside the loop.
527 A Stack trace not printed to standard error.
528-529 null checking added.
530-531 Variables now initialized and declared before use.
532-533 Assert statements deleted.
534 The code no longer outputs a stack trace.
535 There is no backupDatabase call.
536 printStackTrace has been deleted.
537-551 Assert statements deleted.
552 There is no finally but bis is closed in the normal flow of execution.
553 InputStream is passed in so the caller should close it.
554 There is no call to validateFile that has InputStream as a parameter.
555-556 There is no marshal() or unmarshal() call.
557-559 Assert and finally code have been deleted.
560 The exception is not logged.
561 BufferedInputStream is not closed.
562-567 Agree with comment.
568 It is unclear where length is cast to int.
569-571 Agree that calling rollbackTrans in finally may not be appropriate.
572 length is not referenced in the method.
573-575 Agree that calling rollbackTrans in finally may not be appropriate.
576 File not provided with review.
577 No logging was added.
578-582 It calls safeAdd, which we presume prevents overflows.
583 File not provided with review.
584 Can't verify but comment seems reasonable.
585-598 Minor non-security related style/comment/initialization issues.
599 The second declaration of str was removed.
600 Minor non-security related style/comment/initialization issue.
601 The second declaration of str was removed.
602 Case statement was replaced.
603-626 Minor non-security related style/comment/initialization issues.
627 Lines number don't match. Didn't see any possible array bounds violations.
628-674 Minor non-security related style/comment/initialization issues.
675-676 Added null checking.
677-678 Minor non-security related style/comment/initialization issues.
679-681 Added null checking.
682-687 Minor non-security related style/comment/initialization issues.
688 Added null checking.
689 Minor non-security related style/comment/initialization issue.
690 Added null checking.
691-695 Minor non-security related style/comment/initialization issues.
696-697 Added null checking.
698-718 Minor non-security related style/comment/initialization issues.

719 Code was fixed to check correct pointer.
720-721 Minor non-security related style/comment/initialization issues.
722 Else has been added.
723 Code doesn't seem to fit what the rest of the function is performing. Agree with comment.
724 Agree with comment.
725-742 Agree with missing else.
743 220-DBS-FILE is no longer in the file.
744-762 The samples inspected are missing the else.
763-846 Cobol automatically protects against string overflows.
847 Minor non-security related style/comment issues.
848-856 Cobol automatically protects against string overflows.
857 Minor non-security related style/comment issues.
858 Cobol automatically protects against string overflows.
859 Minor non-security related style/comment issues.
860 Cobol automatically protects against string overflows.
861-877 Minor non-security related style/comment issues.
878-885 Minor non-security related style/comment/initialization issues.
886 File not provided with review.
887-904 Minor non-security related style/comment/initialization issues.
905 The assert() call is no longer in the code.
906-912 Minor non-security related style/comment/initialization issues.
913 The assert() call is no longer in the code.
914-919 Minor non-security related style/comment/initialization issues.
***920 szPath is not initialized and is used in the call to GetModuleFileName().
921-922 Minor non-security related style/comment/initialization issues.
***923 szPath is not initialized and is used in the call to GetModuleFileName().
924-938 Minor non-security related style/comment/initialization issues.
939-940 This was fixed it is now compared to 0 with <.
941-948 Minor non-security related style/comment/initialization issues.
949-950 It has been change to format.com with a specific path.
951-995 Minor non-security related style/comment/initialization issues.

3.3.3 DS200 v.2.7.0.1i

Verified with DS200 (lfs_cots-3.0-rhel30-src,lfs_enhanced-2.7.0.11-src,lfs_graphics-2.7.0.11-src,lfs_kernel-2.6.35.13-src)

9-184 Minor non-security related style/comment/initialization issues.
185 m_ppDeviceNameList is not referenced in the code.
186 Code not provided for review.
187-189 Minor non-security related style/comment/initialization issues.
190-191 Code not provided for review.
192-238 Minor non-security related style/comment/initialization issues.
239-249 Code not provided for review.
250-284 Minor non-security related style/comment/initialization issues.
285 Code not provided for review.

286-414 Minor non-security related style/comment/initialization issues.
415 Function is now void with no return value.
416 Error added to the audit output.
417 The warning is NOT logged.
418 Default case added.
419-420 Minor non-security related style/comment/initialization issues.
421 Audit logging was added.
422 We assume validation is done in the set call.
423 Audit logging was added.
424-425 Minor non-security related style/comment/initialization issues.
426 Code not provided for review.
427-437 Minor non-security related style/comment/initialization issues.
438 Code not provided for review.
439-597 Minor non-security related style/comment/initialization issues.
598-599 Code not provided for review.
600-1304 Minor non-security related style/comment/initialization issues.

3.3.4 DS850 v.2.4.0.1b

No discrepancies were cited.