



Applicable to: LV 8.4.4

Build Number: DM0840.422.01\_00

## Installation Procedure

### Prerequisites:

- Please make sure you take a backup of your EAR file in <jboss\_home>\<profile>\deployment.
- Please make sure your EAR file in your <jboss\_home>\<profile>\deployment and <labvantage\_home>\<application>\<applicationid>\ear are in sync. The deployment EAR is the one currently running, and hence is usually the correct version when there is a discrepancy.
- Please note that the instructions below are written in the Windows directory path style. Modify as required if you are using a Linux based operating system.

### Standalone Patch Instructions:

1. Copy the file Patch2268\_N.zip to C:\Temp, where N is the revision number.
2. Unzip the patch to the C:\Temp\Patch2268\_N folder.
3. Log into the LabVantage Console and navigate to the Utilities section.
4. Click the Apply Installer File link.
5. Using the lookup Open for Patch File, select the C:\Temp\Patch2268\_N.zip file.
6. Click Apply Installer and wait for completion of this process (including any application server specifics such as hot-deploys).
7. Restart the application server

### Cluster Patch Instructions:

1. Stop JBoss on all nodes except for the one you determine to be the "primary" node
2. Apply the patch to the primary node as described in standalone instructions above, except stop the primary node application server after patch installation confirmation (Step 6)
3. Copy the primary node's updated managed EAR to the <jboss\_home>\<profile>\deployment and <labvantage\_home>\<application>\<applicationid>\ear folder of all secondary nodes
4. Once the copy to all other instances is complete, separately wait for each secondary node to completely restart before moving on to the next
5. Restart the primary node and wait until it completely restarts

If you need to reapply a patch, no uninstall steps are necessary. Simply redo the steps above.

## Modified Files List

Java API Class:	sapphire\accessor\ConfigurationProcessor.class
Java API Class:	sapphire\servlet\RestClient.class
Java API Class:	sapphire\util\ForwardUtil.class
Java API Class:	sapphire\util\HttpUtil.class
Java API Class:	sapphire\xml\PropertyList.class
Java Private Class:	com\labvantage\opal\handler\DefaultErrorRenderer.class
Java Private Class:	com\labvantage\opal\qcbatch\QCBatchPool.class
Java Private Class:	com\labvantage\sapphire\DefaultAuthentication.class
Java Private Class:	com\labvantage\sapphire\EncryptDecrypt.class
Java Private Class:	com\labvantage\sapphire\actions\mail\SendMail.class
Java Private Class:	com\labvantage\sapphire\admin\ddt\Custodian.class
Java Private Class:	com\labvantage\sapphire\admin\ddt\User.class
Java Private Class:	com\labvantage\sapphire\admin\propertytree\EditorUtil.class





Java Private Class:	com\\labvantage\\sapphire\\admin\\propertytree\\StringEditor.class
Java Private Class:	com\\labvantage\\sapphire\\admin\\system\\SysToolsPropertyHandler.class
Java Private Class:	com\\labvantage\\sapphire\\admin\\webadmin\\PropertyTreeBuilder.class
Java Private Class:	com\\labvantage\\sapphire\\ajax\\operations\\TestBOXIConnection.class
Java Private Class:	com\\labvantage\\sapphire\\layouts\\modern\\ModernLayout\$DevModeState.class
Java Private Class:	com\\labvantage\\sapphire\\layouts\\modern\\ModernLayout\$NavigationBarMode.class
Java Private Class:	com\\labvantage\\sapphire\\layouts\\modern\\ModernLayout\$StatusBarPosition.class
Java Private Class:	com\\labvantage\\sapphire\\layouts\\modern\\ModernLayout.class
Java Private Class:	com\\labvantage\\sapphire\\modules\\dashboard\\gizmos\\BaseGizmo.class
Java Private Class:	com\\labvantage\\sapphire\\modules\\documents\\Form.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\advancedsearch\\SearchByBasic.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\controls\\FileUploader.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\datachart\\data\\Data.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\dynamicmaint\\action\\SaveSDI.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\list\\List.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\lookup\\FileSystem.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\lookup\\FileView.class
Java Private Class:	com\\labvantage\\sapphire\\pageelements\\maint\\UserProfile.class
Java Private Class:	com\\labvantage\\sapphire\\report\\bo\\SapphireBOUtil.class
Java Private Class:	com\\labvantage\\sapphire\\services\\ConfigurationConstants.class
Java Private Class:	com\\labvantage\\sapphire\\services\\RequestService.class
Java Private Class:	com\\labvantage\\sapphire\\services\\SapphireService.class
Java Private Class:	com\\labvantage\\sapphire\\services\\SecurityService.class
Java Private Class:	com\\labvantage\\sapphire\\services\\WebAdminService.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\NotificationController.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\command\\AjaxRequest.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\command\\Login.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\command\\TagRequestPropertyHandler.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\command\\UploadRequest.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\filter\\RejectRequest.class
Java Private Class:	com\\labvantage\\sapphire\\servlet\\rest\\ConnectionsNameSpaceHandler.class
Java Private Class:	com\\labvantage\\sapphire\\tagext\\JavaScriptAPITag.class
Java Private Class:	com\\labvantage\\sapphire\\tagext\\SDITagUtil.class
Java Private Class:	com\\labvantage\\sapphire\\util\\ant\\AntUtil.class





Java Private Class:	com\labvantage\sapphire\util\images\ImageRef.class
WEB-CORE File:	WEB-CORE\elements\scheduler\scripts\planitemmanager.js
WEB-CORE File:	WEB-CORE\modules\security\testldapconnection.jsp
WEB-CORE File:	WEB-CORE\modules\security\user.js
WEB-CORE File:	WEB-CORE\modules\systools\scripts\sysconfig.js
WEB-CORE File:	WEB-CORE\modules\systools\sysconfig.jsp
WEB-CORE File:	WEB-CORE\modules\systools\wiz_chooseantfile.jsp
WEB-CORE File:	WEB-CORE\modules\systools\wiz_runantfile.jsp
WEB-CORE File:	WEB-CORE\modules\webadmin\nodemaintenance.jsp
WEB-CORE File:	WEB-CORE\modules\webadmin\ptreedefaults.jsp

### Bug Details

VC Bug ID:	0021440
Functional Area:	Security
Description:	After applying patch 2175, entered BO passwords are stored as plain text.
Root Cause:	By default Java supports only 128-bit encryption and Starting with Java 8 Update 161, Java 8 supports unlimited encryption key size. The customer using Java version before Java 8 Update 161.
Resolution:	Updated generateRandomAESKey method of EncryptDecrypt.java to allow max allowable keysize. If maxAllowed size>=256 then 256 else maxAllowedsize.
Add'l Changes:	Updated generateRandomAESKey method of EncryptDecrypt.java to allow max allowable keysize. If maxAllowed size>=256 then 256 else maxAllowedsize.

#### Steps to Reproduce:

No Steps Defined.

### Bug Details

VC Bug ID:	0019649
Functional Area:	Core
Description:	ConcurrentModification Exceptions are thrown by various class files.
Root Cause:	Some places in the code were not threadsafe.
Resolution:	Fixed the code to apply synchronization and make them threadsafe.
Add'l Changes:	com.labvantage.sapphire.pageelements.datachart.data.Data com.labvantage.sapphire.tagext.JavaScriptAPITag com.labvantage.sapphire.services.SecurityService com.labvantage.opal.qcbatch.QCBatchPool

#### Steps to Reproduce:

Note: Does not have reproducible steps as the errors rely upon exact timing to be reproduced.

1. Have more than one process try to access the same object simultaneously.

Note: Error in the log depends on the class files involved.





### Bug Details

VC Bug ID: 0020991

Functional Area: Web Security

Description: The application allows redirecting the user to arbitrary locations.

Root Cause: In the redirect forward form, The form action attribute value containing nextpage is rendered without html attribute escape.

Resolution: Insert SafeHtml.encodeForHTMLAttribute call to wrap all form attribute values.

Add'l Changes: FowardUtil.java

Steps to Reproduce:

No steps defined

### Bug Details

VC Bug ID: 0020988

Functional Area: Web Security

Description: A unprivileged user can create a user in the system assign higher level privileges

Root Cause: An authenticated regular user with sophisticated skill can hack the user creation maint form to create a new user.

Resolution: Server handling submitted form validate the user has Administrator or WebPage\_Admin role or has Security Module to allow create or edit Users.

Add'l Changes: TagRequestPropertyHandler.java  
SaveSDI.java

Steps to Reproduce:

No steps defined

### Bug Details

VC Bug ID: 0021064

Functional Area: Web Security

Description: The file system navigators security can be bypassed

Root Cause: Security issues with Serverside File Browser. Hacker is able to bypass the path validation in parent frame and navigate server side paths.

Resolution: This is further enhancing the earlier security token fix. This fix involves sending all the path validation properties from the parent to the child frame and then validating any paths against this information. The path information is placed in an object (this includes the file locations, the permitted browsing and root path) and then is cached for that user using a secure token to identify that cache. Then in the innerframe it first validates it has the secure token and can find the cached object (note that the token was bypassed by the hacker in the first patch given to roche), but then it also checks the path passed in against the secure information in that object (additional level of security). This means that even if a hacker manages to find the secure token and pass that through to the child frame it still wont allow just any path to be passed in and only the paths valid for that browser (i.e. those set up in





the file location policy).

Additional change was also to introduce a master switch to turn off browsing of the server side file system all together.

For both AC patch you can use a new allowserversidebrowsing property in sysconfig and a value of N to disable file browsing.

**Add'l Changes:**

In all versions of this change we have introduced a new allowserversidebrowsing property in sysconfig. When a new row is added in sysconfig with the propertyid of allowserversidebrowsing and the value of N (default Y) then it will also disable the serverside file browsing and the child frame.

**Steps to Reproduce:**

No steps defined

### Bug Details

VC Bug ID: 0021015

Functional Area: Web Security

Description: Add a security switch to disable/enable the RunANT script page.

Root Cause: Security enhancement. Currently the RunAnt functionality can be used through the Run Ant wizard to execute malicious code.

Resolution: Different level of changes depending on release. For 8.4 MR (head) and 8.5 (mainline) we have introduced both a master switch by adding "allowrunant" property to sysconfig table and setting it to N to fully disable the Run Ant wizard, as well as add a security policy setting "runant.runantenabled" which set to N will disable the Run Ant wizard. However on AC patch we have only introduced the sysconfig property "allowrunant" (set to N) to disable the Run Ant functionality and not introduced the security policy setting.

Add'l Changes: In 8.4 MR and 8.5 there is a new security policy setting "runant.runantenabled" which is set to Y by default.

**Steps to Reproduce:**

No steps definid.

### Bug Details

VC Bug ID: 0020829

Functional Area: Web Security

Description: Unprivileged user can modify another user's preferences

Root Cause: Implementation: General Error

Resolution: Server side saving preference ignores submitted userid and always uses the current userid so that the preference changes always saved for the current user

Add'l Changes: TagRequestPropertyHandler.java

**Steps to Reproduce:**

Contact Support for steps.





### Bug Details

VC Bug ID: 0020989

Functional Area: Web Security

Description: Notification Controller servlet allows ajax calls backs

Root Cause: Content type set to HTML text.

Resolution: Changed content type to JSON.

Add'l Changes: None

Steps to Reproduce:

No steps defined.

### Bug Details

VC Bug ID: 0020659

Functional Area: Web Security

Description: The session cookie does not have the SameSite attribute set.

Root Cause: The samesite attribute is relatively new security feature for browser and is not set for connectionid cookie

Resolution: Setting samesite attribute for connectionid cookie to be Strict to mitigate CSRF attack

Add'l Changes: HttpUtil.java

Steps to Reproduce:

No steps defined

### Bug Details

VC Bug ID: 0021163

Functional Area: Web Security

Description: PingRset ajax command has XSS vulnerability

Root Cause: Was missing JSON headers.

Resolution: Added content type header

Add'l Changes: None

Steps to Reproduce:

No steps defined

### Bug Details

VC Bug ID: 0021164

Functional Area: Web Security

Description: Unprivileged user can alter and save the LDAP url in External authentication configuration





Root Cause:	User access to property tree maintenance is controlled by security roles but user's security roles are not validated again on saving. If an authenticated user is also a skilled hacker with access to html source of property tree maint page, the hacker could submit the same form to modify property value.
Resolution:	Checking the user has Administrator or WebPage-admin role or has security module before allow saving of External Authentication, Password Validator and policies
Add'l Changes:	WebAdminService.java
Steps to Reproduce:	No steps defined

## Bug Details

VC Bug ID:	0021255
Functional Area:	Web Security
Description:	XSS is possible with batch templateid input and report description and location inputs
Root Cause:	Specific places user input data are rendered in html without escaping
Resolution:	Added html escape wrapper in those specific places
Add'l Changes:	DeferredErrorRenderer.java SDITagUtil.java List.java
Steps to Reproduce:	No Steps Defined

## Bug Details

VC Bug ID:	0021308
Functional Area:	Storage
Description:	Successful message displayed wrongly , if you Saved any operation in File Sample Page , Manage Package Contents Page ,Unpack Package Page , File Trackitem page Successful message displayed wrongly , if you Saved any operation in File Sample Page , Manage Package Contents Page ,
Root Cause:	previous fix to LV-50738 incorrectly escapes success message html
Resolution:	Not escape success message html
Add'l Changes:	DefaultErrorHandler.java
Steps to Reproduce:	Instance 1 1. Navigate to File Sample Page 2. Choose a Target Storage unit as Box 3. Select a Sample and Auto File 4. Save it.

Note : Operation successful message is appeared . looks like below.







## Messages

## Information

1) Information Operation successful

2) Pick List 1 item has been successfully added to picklist.<input id='\_picklistitems' style='display:none' value='TI-0000096'><input id='picklistsourcesdcid' style='display:none' value='Sample'><input id='\_picklistsoucekeyid1' style='display:none' value='S-200624-00085'>

Pick list section is displayed all the Trackitems.

same issue exists for Manage Package Content

## Instance 2

1. Navigate to LIMS Menu > Monitor Samples > Locations and create a location and add one scheduling plan under "Location Scheduling" tab.
2. Navigate to LIMS Menu > Monitor Samples > Add Schedule Groups and create a schedule group of 'Environment' type and add the location to it.
3. Navigate to LIMS Menu > Monitor Samples > Schedule Groups and edit the schedule group.
4. Click on <Execute Now>.

Note: Success message appears along with some html code -> "1/1 Plan Item(s) executed successfully. Monitor group <monitor group id> Monitor group <a href="JavaScript:top.sapphire.page.navigate('rc?command=page&page=LV\_MonitorGroupMaint&sdcid=LV\_MonitorGroup&keyid1=<monitor group id>');"><monitor group id></a> (refer "Schedule Group\_Issue.png")

## Bug Details

VC Bug ID: 0021109

Functional Area: Console

Description: Installation of security patch 2175 removes the WSPServlet settings within the web.xml file

Root Cause: The patch unnecessarily includes web.xml

Resolution: Remove web.xml from the patch

Add'l Changes: Removed web.xml from patch 2204. No code changes

## Steps to Reproduce:

1. Install LV Connect on a 8.4.1 system.
2. On restart check the web.xml is correct and the wsp is available.
3. Install the Security patch 2175.
4. Check the web.xml file.
  - note the WSP Servlet entries are no longer available and on restart of application the wsp is no longer found.
5. Restore original LV 8.4.1 installation.
6. Install LV Connect.
7. On restart check the web.xml is correct and the wsp is available.
8. Install different patch – ie Patch2072.
9. On restart check the web.xml is correct and the wsp is available.







10.Install the Security patch 2175.

11.Check the web.xml file.

- note the WSP Servlet entries are no longer available and on restart of application the wsp is no longer found.

### Bug Details

VC Bug ID: 0021309

Functional Area: Reflex Rules

Description: LIMS Menu - Monitor Sample - Locations - Selected Value of lookup page is not getting populated in the textbox after select & return  
LIMS Menu - Monitor Sample - Locations - Selected Value of lookup page is not getting populated in the textbox after select & return

Root Cause: Previous fix to escape html input tag attribute broke the specific places because the javascript make ajax call to get html and manipulated as string before set it into page.

Resolution: Handle the special case in the js ajax callback function with the html attribute escapes

Add'l Changes: planitemmanager.js

Steps to Reproduce:

- > Login to application
- > Navigate to LIMS Menu -> Monitor Sample -> Locations
- > Create a location with all mandatory details
- > Navigate to recurring task column of Scheduling detailment tab
- > Choose "Add Sample Using Template" value from the dropdown option
- > Click on the "+" sign under Recurring Task Details Column
- > Select User Existing radio button and click on lookup icon beside it
- > Choose "Raw Material" from the Select Template Page And Click on Select & Return Button

Note :: Value is not getting populated in the textbox beside lookup icon and it is showing error like "Could not execute button.

Cannot read property 'split' of undefined" while click on ok button.

### Bug Details

VC Bug ID: 0020655

Functional Area: Web Security

Description: The application allows redirecting the user to arbitrary locations.

Root Cause: In the redirect forward form, The input parameter hidden field value attributes rendered without html attribute escape.

Resolution: Insert SafeHtml.encodeForHTMLAttribute call to wrap all values.

Add'l Changes: FowardUtil.java

Steps to Reproduce:

No steps defined

### Bug Details





VC Bug ID:	0020653
Functional Area:	Web Security
Description:	Cross-Site Request Forgery (CSRF) The requests sent to the server that trigger actions do not contain a CSRF token and can therefore be entirely predicted.
Root Cause:	Form submitted by file command is not checked for csrftoken correctness. The file update form triggered by dropping a file into file lookup field does not have csrftoken protection
Resolution:	Check file command form for correct csrftoken and always render csrftoken in the form update multipart form and check for csrftoken correctness in the fileupload command in the parsed multipart file upload form.
Add'l Changes:	RejectRequest.java FileUploader.java UploadRequest.java
Steps to Reproduce:	No steps defined

### Bug Details

VC Bug ID:	0020652
Functional Area:	Web Security
Description:	The application allows injecting SQL statements, which are executed by the database for image parameters.
Root Cause:	Possibility of passing sql injection through image request.
Resolution:	Changed sdirequest to use keyid1 rather than querywhere.
Add'l Changes:	None
Steps to Reproduce:	No steps defined

### Bug Details

VC Bug ID:	0020651
Functional Area:	Web Security
Description:	Cross-Site Scripting (XSS) The user's input data is not properly encoded when being echoed back to the user for nc and last search. Therefore, this data can be interpreted as executable code by the browser.
Root Cause:	The nc path Notification Controller servlet used in internal notification mechanism is not configured to go through request security filter in web.xml and the last search text by the same user is rendered without escape html.
Resolution:	Added RejectRequest filter mapping for Notification Controller and encode the last search text by the same user for html attribute
Add'l Changes:	web.xml SearchByBasic.java





Steps to Reproduce:

No Steps defined

### Bug Details

VC Bug ID: 0020606

Functional Area: Security

Description: In System Configuration the mail settings password encryption require stronger encryption level.

Root Cause: BO/mail password encryption was very weak.

Resolution: Now using Advanced Encryption Standard to encrypt/decrypt BO/mail password. Also not rendering the password in the UI.

Add'l Changes: Now using Advanced Encryption Standard to encrypt/decrypt BO/mail password. Also not rendering the password in the UI.

Steps to Reproduce:

No Steps Defined

### Bug Details

VC Bug ID: 0020587

Functional Area: Reports-BOXI

Description: Business Objects passwords encryption require stronger encryption level.

Root Cause: BO/mail password encryption was very weak.

Resolution: Now using Advanced Encryption Standard to encrypt/decrypt BO/mail password. Also not rendering the password in the UI.

Add'l Changes: Now using Advanced Encryption Standard to encrypt/decrypt BO/mail password. Also not rendering the password in the UI.

Steps to Reproduce:

No steps defined.

### Bug Details

VC Bug ID: 0020598

Functional Area: Security

Description: External Authentication configuration application root user password encryption require stronger encryption level.

Root Cause: The encrypt attribute of a property value uses a custom encryption implementation that is not strong enough

Resolution: Changed encryption to use SunJCE AES encryption

Add'l Changes: EncryptDecrypt.java  
10 more  
Description

Steps to Reproduce:

No Steps defined.





### Bug Details

VC Bug ID: 0020627

Functional Area: Security

Description: Encrypted passwords (users and BO) should not be visible in the browser page source

Root Cause: System was displaying in the viewsource.

Resolution: Not rendering the password in the UI.

Add'l Changes: Not rendering the password in the UI.

Steps to Reproduce:

No steps defined

### Bug Details

VC Bug ID: 0020620

Functional Area: Security

Description: In Polices properties defined as passwords and encryption set to Y require stronger encryption level.

Root Cause: The encrypt attribute of a property value uses a custom encryption implementation that is not strong enough

Resolution: Changed encryption to use SunJCE DES encryption. Also not showing encrypted password in html source

Add'l Changes: EncryptDecrypt.java  
11 more

Steps to Reproduce:

No Steps Defined

### Bug Details

VC Bug ID: 0020621

Functional Area: Security

Description: On maintenance page column input defined as password require stronger encryption

Root Cause: Stored SunJCE one way encrypted password can be seen in html source.

Resolution: Not showing stored encrypted password in html source for UserMaint and CustodianMaint pages where password fields exist

Add'l Changes: SDITagUtil.java  
User.java  
Custodian.java

Steps to Reproduce:

No Steps Defined

### Bug Details

VC Bug ID: 0020736





Functional Area:	Web Security
Description:	Users are able to navigate serverside file system using fetch command from client
Root Cause:	The inner iframe (fileview.jsp) is still vulnerable to attack if not used with the parent filesystem.jsp. The parent JSP is what validates paths and urls and the child JSP accepts the final path. It is therefore possible to hijack this JSP and navigate to other paths.
Resolution:	The solution without a complete rewrite to the fileview.jsp was to tightly couple the parent filesystem.jsp and child fileview.jsp together using a security token. We now generate a security token in filesystem.jsp (random string of 50 characters), store it in the cache and pass the token through the request. The fileview.jsp then checks the token in the request against the token in the cache and immediately clears the cache (token has one single use). If the tokens do not match or is not there it voids the request and displays a blank area. This means that you can no longer examine the request for fileview.jsp and hijack it as a fetch to repeat the request as the token would have changed.
Add'l Changes:	None
Steps to Reproduce:	No Steps defined

## Bug Details

VC Bug ID:	0020646
Functional Area:	Core
Description:	REST API must make changes to be inline with other encryption enhancements and changes in behavior. After making a code inspection of the REST API RestClient class, it was determined that the login functionality has the same password encryption algorithm used in VC Bug 0020598 - External Authentication configuration application root user password encryption requires stronger encryption level. The solution for this bug will be to actually stop encrypting the password. HTTPS is required by policy default for LV REST API call, and will encrypt the entire data packet contents using a superior two-way asynch encryption algorithm.
Root Cause:	Customer identified existing password encryption algorithm as too simple. Especially for REST API, we should be using HTTPS to encrypt entire packet with asymmetric algorithm, so solution here is to remove simple approach and document using HTTPS.
Resolution:	Remove old encrypt algo.
Add'l Changes:	N/A
Steps to Reproduce:	<p>While observing using WireShark or some other IP monitoring tool:</p> <p><b>**1.</b> Attempt to make a HTTP POST /connections endpoint REST call using RestClient</p> <p>2. Note encrypted password (when PostMan or other 3rd party REST client code/apps would send password in the clear). If the symmetric key is obtained, note the password can be decrypted</p>





3. Make call again over HTTPS

4. Note entire packet is encrypted, and public/private keys are unique to the specific system...  
There is no way this packet can be decrypted without supercomputer type processing power.

### Quality Statement

This patch has been tested for specific functionality but has not been through a complete regression test. Due to the nature of patches, LabVantage Solutions, Inc. (LabVantage) makes no representations regarding their use or performance and accepts no liability as a result of the use of this software. This software is provided "AS IS" and "WITH ALL FAULTS". LabVantage provides no warranties either express or implied, including IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall LabVantage have any liability whatsoever for incidental and consequential damage as a result of the performance, use or operation of this software. The customer shall have sole responsibility for adequate protection and back-up of data used in conjunction with this software patch.

This signed Certificate signifies acceptance of the patch by the LabVantage Quality department.

Pursuant to our life cycle processes and procedures, this patch is built from our source code control versioning system.

Quality has reviewed testing of the patch and found it adequate and appropriate to ensure that the defect(s) have been remedied as reported as in the Description and Resolution sections. These components are tested to perform in accordance to the documented quality management system of LabVantage.

Project audited and certified by: