GE Healthcare

Invasive Cardiology Security Website
Interventional - Invasive Cardiology

Product Group:	Interventional Invasive Products
Products:	Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, SpecialsLab and ComboLab IT/XT/XTi Recording Systems, Centricity Cardiology Data Management Systems
Version:	6.9.6 Release 3
Subject:	Security Information
Date:	16 May 2019

Summary
The following information is provided to GE Healthcare Technologies customers in regards to known technical security vulnerabilities associated with Mac-Lab® Hemodynamic, CardioLab® Electrophysiology, SpecialsLab and ComboLab IT Recording Systems for Cath Lab, EP Lab and other interventional labs as well as the Centricity® Cardiology Data Management Systems.

Security Patch Base Configuration
The security patch base configuration of the Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi product at release is listed within the MLCL Base Configuration under the Hemodynamic, Electrophysiology and Cardiovascular Information Technologies section of the http://www3.gehealthcare.com/en/Support/Invasive_Cardiology_Product_Security website.

Process
The following actions are taken whenever Microsoft/OEMs releases new security patches:
- The Invasive Cardiology Engineering Team performs a security analysis process for supported Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, GE Client Review and INW Server hardware/software.
- If a vulnerability meets Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi validation criteria, the vulnerability is communicated through the GEHC Product Security Database and Invasive Cardiology Security Website within Three weeks of the patch release.

- Upon validation of the Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi vulnerability, the GEHC Product Security Database and Invasive Cardiology Security Website and affected Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi Security Patch Installation Instructions are updated.

The Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi vulnerability validation criteria are as follows: Any vulnerability that allows malware to alter or deny Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi functionality and/or infect and propagate through normal system use.

Customers are responsible to stay informed with Microsoft vulnerability notifications and to visit the Invasive Cardiology websites to understand the Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi impact. Once a security patch is validated, customers are responsible for the installation of security patches. All Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi Security Patch Installation Instructions are available on the Invasive Cardiology Security Website below the Validated Patches table.

Vulnerabilities exposed after the Mac-Lab IT/XT/XTi and CardioLab IT/XT/XTi product release which do not meet the criteria to be validated are not listed within the GEHC Product Security Database and Invasive Cardiology Security Website. These vulnerabilities are deemed to be non-critical and/or outside normal clinical workflow of the Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi and Centricity INW systems and will not be validated. Unlisted patches should not be installed on the products in order to eliminate malfunction and breakdown risks.

CONTENTS

GE Healthcare

Revision History

Revision	Date	Comments
1.0	22 September 2017	6.9.6 document separation - Qualified KB4025341 - July Monthly Rollup - Added 6.9.6 Installation paths for simplifying patches installation - September Unqualified Patches
2.0	13 October 2017	Added instructions to Disable SMB1 Protocol
3.0	27 October 2017	October Unqualified Patches
4.0	20 November 2017	Added October Qualified Patches
5.0	11 December 2017	November Unqualified Patches
6.0	20 December 2017	For October monthly patch, statement added to uninstall previous monthly patches prior to installation of October monthly patch on the server
7.0	26 January 2018	Qualified November and December monthly rollups with other patches. Also added January Unqualified patches
8.0	9 March 2018	- Added Unqualified February Patch - Qualified minimum password length changes - Changed verbiage from "Patch Refresh" to "Patch Updates"

		• Further MLCL System Security Recommendation
9.0	20 April 2018	• Added January, February, March and April Qualified Patches • Updated "Further MLCL Systems Security Recommendations" section and moved the section Optional Security Updates
10.0	30 April 2018	• Added "Optionally Remove Abode Reader on INW Server" section to the optional section • Added Unqualified April Patch
11.0	17 May 2018	• Added May Qualified Patches • Added .NET patches for versions 3.5 SP1, 4.5.2 • Added Microsoft Office Patches
12	29 June 2018	• Added Unqualified June Patch
13	5 September 2018	• Added Unqualified August Patch
14	18 September 2018	• Qualified June, July, August and September Patches • Qualified .Net Framework Patches • Qualified Microsoft Office 2010 Patches • Qualified Z440 BIOS update • Qualified ML350 Gen9 BIOS update
15	5 December 2018	• Added Unqualified October Patch
16	5 March 2019	• Added Unqualified November 2018, December 2018, January 2019 and February 2019 Patches • Added .NET unqualified patches
17.0	26 March 2019	• Added Unqualified March 2019 Patches
18.0	16 May 2019	• Added instructions to disable Remote Desktop Services for CVE-2019-0708 vulnerability

Installation of the Security Patches on MLCL systems

Requirements:
- Updates may be applied at any time other than while the Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi or SpecialsLab application is open.
- Updates must be re-applied if the system is re-imaged.

- Updates apply to both networked and standalone systems.
- Best practice is to update all applicable MLCL systems at the site.

This document applies to 6.9.6R3 only. Please verify that you are running 6.9.6 using the following procedure before proceeding:

1. Launch the Mac-Lab CardioLab application.
2. Select *Help > About Mac-Lab* (or *CardioLab*, as applicable).
3. Verify the version number is **6.9.6 Release 3**.
4. Click *Close*.
5. Close the application.

Recommendation: <u>Use Internet Explorer (IE) for Catalog download</u>. If you are using the cart feature to download patches, to see the cart it requires opening another tab or new window for http://catalog.update.microsoft.com

How to Log On to Acquisition and Review Systems

When starting up an Mac-Lab, CardioLab or SpecialsLab Acquisition or Review system, an auto-logon sequence starts and automatically logs on to the operating system. To install a security patch, the user must be logged on as **mlcltechuser**.

NOTE: Password information is contained within the Security Guide Manual. Otherwise, contact the system administrator or GE Technical Support for current password information.

1. Power on the Acquisition system.
2. The system boots up to the *Custom Shell* screen.
3. Press **Ctrl + Action + Del**.
4. Click *Logoff*. On Windows XP, click *Logoff* again.
5. Click *OK*.
6. Immediately hold down the **Shift** key until the login window is displayed.
7. Log on to the operating system locally as **mlcltechuser**.
8. Log on to the *Custom Shell* locally as **mlcltechuser**.

How to Log On to the Centricity Cardiology INW Server

GE Healthcare

Password information is contained within the Security Guide Manual. Otherwise, contact the system administrator or GE Technical Support for current password information. Logon to the INW Server as **administrator**

How to Log On to MLCL Software Only Systems

Since Software Only systems are supported by the customer, the system needs to be logged into with an **administrator** account.

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

We are in the process of qualifying the patch that addresses this vulnerability however, we recommend as a mitigation, that the RDS/Terminal Service is disabled on all ML/CL systems. Refer to the instructions below on disabling the service.

Disable Remote Desktop Services on Windows 7
On Windows 7, do the following to disable Remote Desktop Services:

1. Right-click on *Computer* and select *Properties*
2. On the *System* window, click *Remote settings*
3. Uncheck the following option if it is checked:
   Allow Remote Assistance connections to this computer
4. Select the following option if it is not already selected:
   Don't allow connections to this computer
5. Click *OK* to close the *System Properties* window
6. Click *Start* > *Control Panel* > *Administrative Tools* > *Services*
7. Double-click on the entry for **Remote Desktop Services**
8. Set the *Startup type* to *Disabled*
9. Click *OK* to close the *Remote Desktop Services Properties* window
10. Reboot the system

NOTE: The Multi-space option workflow within the Workspace Integration will be unavailable after disabling Remote Desktop Services.

Disable Remote Desktop Services on Windows 2008 R2

On Windows Server 2008 R2, do the following to disable Remote Desktop Services:

1. Right-click on *Computer* and select *Properties*

2. On the *System* window, click *Remote settings*

3. Uncheck the following option if it is checked:
   Allow Remote Assistance connections to this computer

4. Select the following option if it is not already selected:
   Don't allow connections to this computer

5. Click *OK* to close the *System Properties* window

6. Click *Start* > *Administrative Tools* > *Services*

7. Double-click on the entry for **Remote Desktop Services**

8. Set the *Startup type* to *Disabled*

9. Click *OK* to close the *Remote Desktop Services Properties* window

10. Reboot the system

How to Install Printer Firmware

The system which will apply the firmware to the printer should be provided by the customer.
NOTE: Mac-Lab CardioLab system should not be used to download and/or apply the Printer Firmware.
- Follow the download link in the table
- Select the appropriate printer
- Select English and the applicable MLCL operating system
- Select English and under the Firmware category select the applicable Firmware Update Utility and Click Download
- Launch the firmware installer and follow the instructions to complete the firmware update

How to Update Intel Management Engine Firmware (HP Z440) – HPSBHF03557 Rev. 1

1. Logon to the Windows OS and MLCL *Custom Shell* as **mlcltechuser**.
2. Navigate to the location within the section, *MLCL V6.9.6 Patch Updates*, which has the Intel Management Engine Firmware Update file **sp80050.exe**.
3. Right-click on the **sp80050.exe** file and select *Run as administrator*.
4. Click *Yes* on the User Account Control dialog box.
5. Click *Next* on the InstallShield Wizard.
6. Accept the agreement and click *Next*.
7. Press **Y** on the command prompt which states "Do you want to update the Management Engine Firmware now [Y/N]?
8. Reboot the system once the firmware update is completed.

Steps to verify the firmware update was successful:

1. After system reboots, within the HP screen press **F10** to enter setup menu.
2. Go to *Main > System Information*.
3. The ME Firmware Version should be at *9.1.41.3024*.

Z440 BIOS Update to v2.34 Instructions:

1. Go to the HP Customer Support - Software and Driver Downloads website:

   https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828
2. Select *BIOS*.
3. Select *Download* for HP Z440/Z640/Z840 Workstation System BIOS 2.34 Rev.A.
4. Log on to the z440 computer as *administrator*.
5. Run the downloaded *sp80745.exe* file.
6. Select *Yes* to allow.
7. Select *I accept the terms in the license agreement*.
8. Select *View Contents of the HPBIOSUPDREC folder*. This opens folder:

   C:\\swsetup\SP80745\HPBIOSUPDREC
9. Run *HPBIOSUPDREC.exe*.

10. Select *Yes* to allow.
11. After several seconds, a log file is created and an install utility window appears. Select *Update* and *Next*.
12. Follow the onscreen instructions, select *Restart*.
13. The BIOS update will take a few minutes, do not remove power during update. The computer will Reboot twice during this update.
14. After the update, on the first boot screen before Windows launches, verify the BIOS version 2.34 on the bottom left of the screen appears.

Z440 BIOS Update to v2.45 Instructions:

1. Go to the HP Customer Support - Software and Driver Downloads website:

   https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828
2. Select *BIOS*.
3. Select *Download* for HP Z440/Z640/Z840 Workstation System BIOS 2.45 Rev.A.
4. Log on to the z440 computer as *administrator*.
5. Run the downloaded *sp88253.exe* file.
6. Select *Yes* to allow.
7. Select *I accept the terms in the license agreement*.
8. Select *View Contents of the HPBIOSUPDREC folder*. This opens folder:

   C:\\swsetup\SP88253\HPBIOSUPDREC
9. Run *HPBIOSUPDREC.exe*.
10. Select *Yes* to allow.
11. After several seconds, a log file is created and an install utility window appears. Select *Update* and *Next*.
12. Follow the onscreen instructions, select *Restart*.
13. The BIOS update will take a few minutes, do not remove power during update. The computer will Reboot twice during this update.
14. After the update, on the first boot screen before Windows launches, verify the BIOS version 2.45 on the bottom left of the screen appears.

ML350 Gen9 BIOS Update to v2.56 Instructions:

1. Go to the HP Customer Support - Software and Driver Downloads website:
   https://support.hpe.com/hpsc/swd/public/detail?swItemId=MTX_116f29414b06465c96e6bd94ae
2. Select *Download* for HP ML350 Gen9 Server BIOS 2.56

3. Log on to the ML350 Gen9 Server as **administrator**.
4. Run the downloaded **cp034882.exe** file.
5. Click on **Run**
6. Click on **Install**
7. Follow the onscreen instructions, select **close** after installation is complete.
8. Select **Yes** to reboot.
9. The BIOS update will take a few minutes, do not remove power during update.
10. After the update, on boot screen before Windows launches, verify the BIOS version 2.56 on the bottom left of the screen appears.

ML350 Gen9 BIOS Update to 5/21/2018 Instructions:

1. Go to the HP Customer Support - Software and Driver Downloads website:
   https://support.hpe.com/hpsc/swd/public/detail?sp4ts.oid=1009483731&swItemId=MTX_2fad1bbda82e4d5ca0673a1b43&swEnvOid=4184
2. Select **Download** for HP ML350 Gen9 Server BIOS 5/21/2018
3. Log on to the ML350 Gen9 Server as **administrator**.
4. Run the downloaded **cp035797.exe** file.
5. Click on **Run**
6. Click on **Install**
7. Follow the onscreen instructions, select **close** after installation is complete.
8. Select **Yes** to reboot.
9. The BIOS update will take a few minutes, do not remove power during update.
10. After the update, on boot screen before Windows launches, verify the BIOS version 5/21/2018 on the bottom left of the screen appears.

OPTIONAL – How to Install INW Server Performance Enhancement

The following patches do not resolve security vulnerabilities and are optional. These patches may improve network performance. The installation procedure below must be followed and all listed patches deployed together. This deployment may take up to 12 hours, the large percentage within the KB2775511 installation.

1. Using a non-MLCL system, visit and download the following patches to removable media.

Visit http://catalog.update.microsoft.com/ and enter the below KB numbers to access the patches.
KB2775511 - http://support.microsoft.com/kb/2775511
KB2732673 - http://support.microsoft.com/kb/2732673
KB2728738 – http://support.microsoft.com/kb/2728738
KB2878378 – http://support.microsoft.com/kb/2878378

The following patches are summarized at KB2473205 - https://support.microsoft.com/en-us/kb/2473205
KB2535094 – http://support.microsoft.com/kb/2535094 Download at - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2535094&kbln=en-us
KB2914677 – http://support.microsoft.com/kb/2914677 Download at - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2914677&kbln=en-us
KB2831013 – http://support.microsoft.com/kb/2831013 Download at - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2831013&kbln=en-us
KB3000483 – http://support.microsoft.com/kb/3000483 Download at - http://catalog.update.microsoft.com/
KB3080140 – http://support.microsoft.com/kb/3080140 Download at - http://catalog.update.microsoft.com/
KB3044428 – http://support.microsoft.com/kb/3044428 Download at - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=3044428&kbln=en-us

2. Log on to the INW Server as **Administrator**.
3. Insert the removable media and install the patches in the order listed above.
4. Follow the Microsoft installation instructions to complete the installation of the patches.
5. Select **Windows Start -> Run** and enter **Regedit** and Enter.
6. In **Regedit** window, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip**
7. In the dialog Menu, select **File -> Export**. Name the file **MLCLRegSave.reg** and place in the **C:\Temp** directory.
8. In Regedit windows, from **Tcpip** navigate to **Parameters**.
9. In the dialog Menu, select **Edit -> New -> DWORD (32-bit) Value**. A new entry is created and name it **'MaxUserPort'**.
10. Right click on **'MaxUserPort'**, select **Modify** and enter the value **65534** with a base of **Decimal**.
11. Follow the same procedure above and create a new entry named **'TcpTimedWaitDelay'.** Enter the value **60** with a base of **Decimal**.
12. Exit the **Regedit** dialog.
13. Reboot the INW Server.

OPTIONAL – How to Install Plugin 20007 – Disable SSL V2/V3 – KB187498

1. Log on to Windows as **Administrator** or a member of that group.
2. Open a command prompt and enter the following commands:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0" /f

4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
5. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
6. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" /v Enabled /t REG_DWORD /d 00000000 /f
7. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0" /f
8. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /f
9. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
10. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v Enabled /t REG_DWORD /d 00000000 /f
11. Close the command prompt.

OPTIONAL – How to Install Plugin 35291 –Weak Hashing

1) Load your security certificate in SQL Server on each ML/CL system in the network (server, acquisitions, reviews and virtual reviews) or the ML/CL standalone acquisition.
2) Disable RDP on each member of the network.
   a) My Computer>Properties>Remote settings>Remote
   b) Check "Don't allow connections to this computer".
   c) Click ok and reboot.

OPTIONAL – How to Install Plugin 65821 –SSL RC4 Cipher Suites Supported

1. Log on to Windows as **Administrator** or a member of that group.
2. Open a command prompt and enter the following commands:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" /f
4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" /v Enabled /t REG_DWORD /d 00000000 /f
5. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128" /f

6. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128" /v Enabled /t REG_DWORD /d 00000000 /f
7. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128" /f
8. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128" /v Enabled /t REG_DWORD /d 00000000 /f
9. Close the command prompt.

OPTIONAL – How Remove Vulnerability for Plugin 63155 – Microsoft Windows Unquoted Service Path Enumeration

1. Log on to Windows as Administrator or a member of that group
2. Open Regedit do the following
    a. On Windows 7
        i. Navigate to HKLM\System\CurrentControlset\Services\RtkAudioService
        ii. Change the imagepath key value from:
            C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe
             To:
            "C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe"
            Note: The leading and trailing Quote marks are part of the key value. The quotes are what removes the vulnerability

    b. On Windows 2008R2
        i. Navigate to HKLM\System\CurrentControlset\Services\Gems Task Scheduler
        ii. Change the imagepath key value from:
            C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe
            To:
            "C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe"
            Note: The leading and trailing Quote marks are part of the key value. The quotes are what removes the vulnerability

OPTIONAL – How to Disable the SMB1 Protocol

1. Log on to Windows as **Administrator** or a member of that group.
2. Open a command prompt and enter the following commands:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /f
4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v SMB1 /t REG_DWORD /d 00000000 /f
5. sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
6. sc.exe config mrxsmb10 start= disabled

Patch Links

The patches displayed below are qualified on an independent basis and can be installed on a one-by-one basis, although it is recommended that all qualified patches are installed. There are dependencies within the qualified patch list. In the table below, it is recommended the patches are installed in order from top to bottom to ensure all pre-requisites are met for all patches. On occasion the patch dependencies require system reboots which are identified in the table below.

NOTE: Due to site configurations, system patch set, qualified patches which have been installed previously or patch dependencies, some patches could fail to install due to the functionality is already installed. The Microsoft patch installer will alert you to this issue. It this occurs, please continue with the next patch installation.

Alternate Patch locations: In early 2016 Microsoft announced that some patches would no longer be available on the Microsoft Download Center https://blogs.technet.microsoft.com/msrc/2016/04/29/changes-to-security-update-links/ Therefore, some of the links provided below may not work. Microsoft may move/remove these links at any time without notice. However, if the links do not work, there are two alternate methods for downloading patches. The first is the Microsoft Catalog http://catalog.update.microsoft.com . Most fixes not on Microsoft Download Center will be available from the Microsoft Catalog. If a fix is not available from the Microsoft Catalog, Microsoft has monthly ISO files of the security updates available at https://support.microsoft.com/en-us/kb/913086 To use the ISOs, determine the month of the patch, download the applicable ISO and extract the patch. If after exhausting all three methods, you are still unable to obtain a patch, please contact GE Technical Support for further assistance.

6.9.6 Installation Paths

There are multiple installation paths depending on the version of 6.9.6 installed and any previous patches which have been installed. The following information will help guide you through correct installation path

Determine which version of 6.9.6 you are running. This can be done from the Mac Lab/Cardio Lab application. Go to Help/About and you will see the Release number. The release number combined with the installation scenario will determine the correct path.

Note: The section MLCL Optional Security Updates can be applied after all other patches/updates have been applied. The optional updates provide additional security but are not required. You may apply some of the optional patches but choose to bypass others. For example, you may want to disable some of the vulnerable protocols by you may not want to address Weak Hashing due to cost and complexity of certificate management. This will not cause problems. However, _**all other updates are strongly recommended**_.

Some updates are documented as **superseded**. These are left in the document for completeness but can be skipped.

The following sample scenarios are provided for reference.

(1) New Setup/Reimage a machine for disaster recovery.
  (a) For R3 Apply the updates from the following section
    (i) MLCL V6.9.6 2017 Patch Updates 1

(2) The machine was setup and initially patched but no subsequent updates have been applied.
  (a) For R3 Apply the updates from the following section
    (i) No further patches are required. The Patch Updates would have been applied as part of setup

(3) The machine was setup and all previous patches have been applied
  (a) For R3 Apply the updates from the following section
    (i) No further patches are required. The Patch Updates would have been applied as part of setup

Unqualified Patches MLCL v6.9.6 R3

	INW Server	Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab	GE Client Review Workstation	Virtual Review
Operating System Platform	Windows Server 2008 R2 SP1	Windows 7 SP1	Windows 7 SP1	Windows 7 SP1
Current Unqualified Vulnerability	KB4462915 (CVE-2018-8320) KB3177467(ADV990001) KB4467106(CVE-2018-8256, CVE-2018-8476) KB4470600 | KB4470493 (CVE-2018-8517) HP Advisory a00040711en_us KB4486564 (CVE-2019-0626) KB4490425(ADV190006) HPESBHF03904 rev.1 HPESBHF03874 rev.1	SP93482 SP91925 KB4467106(CVE-2018-8256, CVE-2018-8476) KB4470600 | KB4470493 (CVE-2018-8517) KB4486564 (CVE-2019-0626) KB4490425(ADV190006) KB3177467(ADV990001) KB4489885(CVE-2019-0683) KB4474419(ADV190009)	SP93482 SP91925 KB4467106(CVE-2018-8256, CVE-2018-8476) KB4470600 | KB4470493 (CVE-2018-8517) KB4486564 (CVE-2019-0626) KB4490425(ADV190006) KB3177467(ADV990001) KB4489885(CVE-2019-0683) KB4474419(ADV190009)	SP93482 SP91925 KB4467106(CVE-2018-8256, CVE-2018-8476) KB4470600 | KB4470493 (CVE-2018-8517) KB4486564 (CVE-2019-0626) KB4490425(ADV190006) KB3177467(ADV990001) KB4489885(CVE-2019-0683) KB4474419(ADV190009)

	INW Server	Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab	GE Client Review Workstation	Virtual Review
	KB4489885(CVE-2019-0683) KB4474419(ADV190009) HPSBHF03572 rev. 4			

MLCL V6.9.6 2017 Patch Updates 1

Windows 7 (Acquisition, Review and Virtual Review)		
KB	**Link**	**Notes**
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB2901907	https://www.microsoft.com/en-us/download/details.aspx?id=42642	Right click and Run as Administrator
Adobe 11.0.20	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191	
KB4025341 July Rollup 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=12c93ad9-ef0e-4ce6-8a1d-84713223d24a	
KB4034664 August Rollup 2017 **Superseded**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e0a94bad-5b2c-4611-9066-24491ce9bb4f	To successfully install this Rollup, you must uninstall July Rollup **KB4025341 and reboot before installing KB4034664**
Reboot Required	-	

KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1daeb6d1-b103-4baa-bbde-5326e17e89e4	Run KB4014514 and KB4014504 only. For KB4014514, right click and Run as Administrator,
KB3125869	https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015	Download and install only the "Enable the User32 exception handler hardening feature in Internet Explorer"
KB2889841	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bb220b30-6d01-4e57-8db6-3e492d6b65d3	
KB3178688	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=322c28f5-349c-468a-ac94-901616f52372	
KB3178690	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=06e2c9fb-65b7-48f5-b6e2-58071f17f9bd	
KB3178687	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=726adfc6-4ac9-4409-bdab-2892b7058e78	
kb3141538	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6be5e673-e3f6-4c8e-8834-732baf0eb5d3	
KB3191847	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4b4bbe2b-a25d-4509-a069-f5efc227b4ad	
KB3191907	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c8533f11-51f9-4f84-96d8-c619947cc7c0	
KB3118310	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c59a1bb2-ff1f-427a-a8d7-2cab1cb3e7d1	
KB3191843	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f715a81d-102d-416a-9a89-e9ebdace0a6d	
KB3191899	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7698c63a-b85f-4647-bcb1-1be0256c3f43	

KB3203468	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	Use all-proof-en-us_......cab
KB3213624	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3658f96e-a521-429d-a9a9-e70e30f5d830	
HPSBHF03557 Rev. 1	ftp://ftp.hp.com/pub/softpaq/sp80001-80500/sp80050.exe	Not applicable for Virtual Review.
HP z440 BIOS Update	https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828	
KB3118378	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ae54ce3d-e321-4831-a1ba-fcae8eb430a0	
<u>Reboot Required</u>	-	
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
Windows 2008R2 (INW)		
KB	Link	
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.20	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191	

KB3125869	https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015	Download and install only the "Enable the User32 exception handler hardening feature in Internet Explorer"
KB4025341 July Rollup 2017	https://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b2423c5b-0254-4747-88bb-ec1a785549cb	
Superseded KB4034664 August Rollup 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=80f7899d-451d-4e3f-b54e-d488a06a3c58	To successfully install this Rollup, you must uninstall July Rollup **KB4025341 and reboot before installing KB4034664**
KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=dedea6da-e039-487b-8ec6-2729551f7165	Run KB4014514 and KB4014504 only. For KB4014514, right click and Run as Administrator,
HPSBMU03653 rev.1	https://h20566.www2.hpe.com/hpsc/swd/public/detail?swItemId=MTX_083799d6dad34195bb47cb43c1	
Reboot Required		
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing] **State=dword:00010000**	
	[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters] **LdapEnforceChannelBinding=DWORD:1**	Apply only on Domain Controller Need starting July Rollup-KB4025341 (CVE-2017-8563)

MLCL V6.9.6 2017 Patch Updates 2

The following patches bring the MLCL system to a more recent patch level and address several security vulnerabilities. The following guidelines apply:

1) The above patches are required patches for 6.9.6 and must be applied first.
2) It is expected that some patches listed will already be on the system.
3) Pay attention to the Notes section for special handling instructions
4) Patches must be applied in order except where indicated.
5) Reboots are only required where indicated. If a Patch requests a reboot at another point, the system can be rebooted but it is not required.
6) Patches will not install if the software component to be patched is not present (such as an IE8 patch on a system that does not have IE8 installed).

Note: KB4041681 replaces KB4041678 for both Windows 7 and Windows Server 2008 R2 to address CVE-2017-11771, CVE-2017-11772, CVE-2017-11780, CVE-2017-11781

Windows 7 (Acquisition, Review and Virtual Review)		
KB	**Link**	**Notes**
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.23	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6279&fileID=6314	
KB4041681 October 2017 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8a346e85-6ae3-46aa-a9e1-2e70e760f61c	
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	

	State=dword:00010000	
	Reboot Required	

Windows 2008R2 (INW Server)

KB	Link	Notes
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.23	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6279&fileID=6314	
KB4041681 October 2017 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=cd0388fd-5aca-4a13-8417-c28e1d8b7dda	**To successfully install this Rollup, you must uninstall July Rollup KB4025341, August Rollup KB4034664 and reboot before applying KB4041681** Make the following Registry Change – Only on Domain Controller if it does not exist: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters] LdapEnforceChannelBinding=DWORD:1 **This registry key is needed on Domain controller** starting July

		Rollup- KB4025341 (CVE-2017-8563)
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing] **State=dword:00010000**	
	Reboot Required	

MLCL V6.9.6 2018 Patch Updates 3

The following patches bring the MLCL system to a more recent patch level and address several security vulnerabilities. The following guidelines apply:

1) The above patches are required patches for 6.9.6 and must be applied first.
2) Pay attention to the Notes section for special handling instructions
3) Patches must be applied in order except where indicated.
4) Reboots are only required where indicated. If a Patch requests a reboot at another point, the system can be rebooted but it is not required.

Follow these steps to make the following registry changes to remediate June and September monthly rollup vulnerabilities.
Reference: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8529

Windows 7 (Acquisition, Review and Virtual Review) & Windows 2008R2 (INW Server):

1. Click **Start**, click **Run**, type **regedt32** or type **regedit**, and then click **OK**.
2. In Registry Editor, locate the following registry folder: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl**
3. Right-click **FeatureControl**, point to **New**, and then click **Key**.
4. Type **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, and then press Enter to name the new subkey.
5. Right-click **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, point to **New**, and then click **DWORD Value**.
6. Type "iexplore.exe" for the new DWORD value.
7. Double-click the new DWORD value named iexplore.exe and change the **Value** data field to **1**.
8. Click **OK** to close.

Windows 2008R2 (INW Server):

1. Click **Start**, click **Run**, type **regedt32** or type **regedit**, and then click **OK**.
2. In Registry Editor, locate the following registry folder: **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl**
3. Right-click **FeatureControl**, point to **New**, and then click **Key**.
4. Type **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, and then press Enter to name the new subkey.
5. Right-click **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, point to **New**, and then click **DWORD Value**.
6. Type "iexplore.exe" for the new DWORD value.
7. Double-click the new DWORD value named iexplore.exe and change the **Value** data field to **1**.
8. Click **OK** to close.

Windows 7 (Acquisition, Review and Virtual Review)		
KB	**Link**	**Notes**
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB4048957 November 2017 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=224b07ab-de98-45f0-8b9c-83551cac66f6	
	Reboot Required	
KB4054518 December 2017 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5b48d1cb-83f7-43e1-9308-18872ffe4dce	
	Reboot Required	
KB3203468	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	

July 2017 Microsoft Office 2010		
KB3213626 September 2017 Microsoft Office 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2bb1487f-b287-41a9-b0ec-01b42aa4759e	
KB3128027 September 2017 Microsoft PowerPoint 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=474aa90a-7767-4f4f-b3f5-2ffa12fea4e6	
KB3141537 September 2017 Microsoft Publisher 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0c646d3e-697d-4463-a6ea-afb3493c5cea	
KB2553338 October 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=14e73852-cbd2-456a-a9a8-7f0c10f1fa40	Might get error message (The upgrade path cannot be installed…) This error message can be ignored.
KB2837599 October 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=54ccbc02-879e-4aa1-b817-12418ce8dfcd	
KB4011612 December 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8230d598-8ab1-4efc-89b6-d3507a6dfd20	Might get error message (The upgrade path cannot be installed…) This error message can be ignored.
KB4011660	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d7594745-04d5-4631-b2d7-289816f4dd43	

January 2018 Microsoft Excel 2010		
KB4011659 January 2018 Microsoft Word 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0b5a1bf0-3043-47fd-afc3-d2fb55a46a96	
KB4011611 January 2018 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3b2c376c-ea57-4925-b81d-3b765d456f2b	Extract to a location and run the extraction to install. Check installed updates for a successful install.
KB4011610 January 2018 Microsoft Office 2010	https://www.microsoft.com/en-us/download/details.aspx?id=56447	
KB4054172 January 2018 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=537fc3ba-4248-40b8-9498-8a671abebfe9	Install the following KB4054172, KB4019990 and KB4054176
KB2719662	Create the following Registry Keys	
	Key=[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\] **Value Name=[TurnOffSidebar]** **Type=[REG_DWORD]** **Data=[1]**	
KB2269637	Create the following Registry Keys	
	Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] **Value Name=[CWDIllegalInDllSearch]** **Type=[REG_DWORD]**	

	Data=[1]	
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

Windows 2008R2 (INW Server)

KB	Link	Notes
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB3177467 Service Stack	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f1b99598-a22d-4fbe-9b63-09724833acc3	**Required for successful Monthly rollup installation without uninstalling previous monthly rollup**
	Reboot Required	
KB4048957 November 2017 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=435d3006-04ae-4c27-a5f9-3c36f09e58ed	
	Reboot Required	
KB4054518	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=09064e30-6f3e-4c99-8d09-fbc2ba06b436	

December 2017 Monthly Rollup		
	Reboot Required	
KB4054172 January 2018 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fdecaf44-50a3-4667-a935-f9e7af0bb317	
KB2269637	Create the following Registry Keys	
	Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] **Value Name=[CWDIllegalInDllSearch]** **Type=[REG_DWORD]** **Data=[1]**	
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

MLCL V6.9.6 2018 Patch Updates 4

The following patches bring the MLCL system to a more recent patch level and address several security vulnerabilities. The following guidelines apply:

1) The above patches are required patches for 6.9.6 and must be applied first.
2) Pay attention to the Notes section for special handling instructions
3) Patches must be applied in order except where indicated.
4) Reboots are only required where indicated. If a Patch requests a reboot at another point, the system can be rebooted but it is not required.

Windows 7 (Acquisition, Review and Virtual Review)

KB	Link	Notes
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB4056894 January 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=63bb3909-e5fe-45a2-8d59-44f9df52317f	
	Reboot Required	
KB4091290	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c70372c5-bd6c-48f7-b562-c326bc1327a4	
KB4074598 February Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=651e95ab-6e7c-4ea6-9cd2-3cbabd9b76f0	
	Reboot Required	
KB4099950	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0872a60d-385a-4486-8322-9e759802017a	**CAUTION: This patch has to be applied before March Monthly rollup KB4088875. Not applying this before March rollup can affect NIC settings.**
KB4088875 March Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3ed75c38-aa36-437e-bf4f-574789591e03	
	Reboot Required	
KB4096040	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=be3cdb55-862c-4362-b015-894e381e07f9	

KB4099467	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f325deb3-28fc-45a3-ab7b-5264f801daf6	
	Reboot Required	
KB4093118 April Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=647f49ef-0f0a-49dc-9766-dd255cded1af	
KB4011707	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=969c78ec-cd6a-4295-ade3-a57ca7f8b3b2	
KB3114874	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9fae99be-ddc3-4e37-b3ee-9b631fd50eca	
KB3114416	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=da77f81d-187b-4cae-a75a-d64766a7713d	
KB4057114	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0aa653a1-1459-44cd-be0b-0fcb77e4ef85	**Install AMD64_X86-en-sqlserver2008-kb4057114-x86_a9295f99a2ee7c714f540f3697be0fd4aee7a7bf.exe** Run from a cmd prompt as Administrator using the following command: AMD64_X86-en-sqlserver2008-kb4057114-x86_a9295f99a2ee7c714f540f3697be0fd4aee7a7bf.exe /ACTION=Patch /INSTANCENAME=MSSQLSERVER /IGNORESERVICERESTARTSTATE
	Reboot Required	
KB4103718 May 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3f4d0c73-a177-48cf-a3e7-97d1a94cba87	
	Reboot Required	

KB4095874 **.NET 3.5 SP1** **and KB4096495** **.NET 4.5.2**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d000d6a2-3321-4381-9a24-3345b2cd0435	KB4099633 is the KB number to use to download and install the patch for KB4095874 and KB4096495. Inside your downloaded file has multiple KBs. Follow these order of installation: 1) Install KB4019990(You may see already installed message for this KB, ignore and continue) 2) KB4095874 3) KB4096495
	Reboot Required	
KB4022146 **Microsoft Excel 2010**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5795d737-4091-4784-a707-007b99d3daef	**KB4022146** **Microsoft Excel 2010**
KB2899590 **Microsoft Office 2010**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d8acdbaf-7f56-4c65-a898-9fdfc7a2d83a	**KB2899590** **Microsoft Office 2010**
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

Windows 2008R2 (INW Server)

KB	Link	Notes
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
CP034882 Firmware Update for ML350 Gen 9 Server	https://support.hpe.com/hpsc/swd/public/detail?swItemId=MTX_116f29414b06465c96e6bd94ae	**Refer to "ML350 Gen9 BIOS Update to v2.56 Instructions" section above for installation instructions**
	Reboot Required	
KB4056894 January 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fc887fd2-cd35-434b-b6e3-1fef99b2e7ce	
	Reboot Required	
KB4091290	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c96d43ea-477f-47a1-919f-6936c8d628a3	
KB4074598 February Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f3ab18cb-219e-4287-b14c-3a05c8d9479a	
	Reboot Required	
KB4099950	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=38b41383-c716-488c-a937-163bf04f6956	**CAUTION: This patch has to be applied before March Monthly rollup KB4088875. Not applying this before March rollup can affect NIC settings.**
KB4096040	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3af42ab1-13ed-42b5-9e4e-a841a71e7f2c	

GE Healthcare

KB4088875 March Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=03df6731-e0a6-4917-9da3-161a0b7f6b09	
KB4099467	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=38800bcc-c954-4822-b864-6ae91cc19bb2	
	Reboot Required	
KB4093118 April Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d2c7363c-323f-4e92-892a-90b83027e4aa	
	Reboot Required	
KB4057114	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0aa653a1-1459-44cd-be0b-0fcb77e4ef85	**Install AMD64-en-sqlserver2008-kb4057114-x64_9ce0b7c5909d8fcc5b9a12d17f29b7864a9df33a.exe file.** Run from a cmd prompt as Administrator using the following command: AMD64-en-sqlserver2008-kb4057114-x64_9ce0b7c5909d8fcc5b9a12d17f29b7864a9df33a.exe /ACTION=Patch /INSTANCENAME=MSSQLSERVER /IGNORESERVICERESTARTSTATE
	Reboot Required	
KB4103718 May 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4fe75106-a2ba-4186-aecd-10424a19225e	
	Reboot Required	
KB4095874	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=62ccd808-b5a5-4be9-8a38-8e2a829e29d1	**KB4099633 is the KB number to use to download and install the**

.NET 3.5 SP1 and KB4096495 .NET 4.5.2		patch for KB4095874 and KB4096495. The downloaded file has multiple KBs. Follow these order of installation: 1) **Install KB4019990(You may see already installed message for this KB, ignore and continue)** 2) **KB4095874** 3) **KB4096495**
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

MLCL V6.9.6 2018 Patch Updates 5

The following patches bring the MLCL system to a more recent patch level and address several security vulnerabilities. The following guidelines apply:

5) The above patches are required patches for 6.9.6 and must be applied first.
6) Pay attention to the Notes section for special handling instructions
7) Patches must be applied in order except where indicated.
8) Reboots are only required where indicated. If a Patch requests a reboot at another point, the system can be rebooted but it is not required.

Windows 7 (Acquisition, Review and Virtual Review)		
KB	**Link**	**Notes**

	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Z440 BIOS Update to v2.45	https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828	**Refer to Z440 BIOS Update to v2.45 Instructions above.**
	Reboot Required	
KB4284826 June 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=326a9830-3983-402d-b48b-7a35f99c516a	
	Reboot Required	
KB4338818 July 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ea409dca-1368-48cf-94c1-d510b1690d74	
	Reboot Required	
KB4338821	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=dafd8f28-09a9-4d17-8a6c-93341a8379ec	
	Reboot Required	
KB4343900 August 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d785f6dd-d90b-4cb9-838a-8faf5971165f	
	Reboot Required	
KB4343894 IE 11	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3fc3f78a-19c5-45bc-9f06-6a14cec0f007	

	Reboot Required	
KB4457144 September 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f5c88de4-720e-4ed1-b95f-6ce4d4d06087	
	Reboot Required	
KB4345590 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=08968031-142d-4dcb-9fd8-29fbd6ae9960	**Install KB4344149 first (restart if prompted) followed by KB4344152**
	Reboot Required	
KB3203468 Microsoft Office Proof 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	
KB4032223 Microsoft Excel 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=cd28cd6b-b3c2-4266-b417-d26d53f7d75f	
KB4227175 Microsoft Excel 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bba3a281-f10f-45bc-adf8-9e4436d4c39b	
KB4018311 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f96028c5-b20a-41a6-9963-83261d690a62	
KB3213636 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7e7049e7-b870-4c87-af60-bc5a0bace002	

KB4022198 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=cc4958f4-308d-474c-a655-567e41cf9b1d	
KB3115197 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=393d97f5-b447-43c5-9e0c-b6707c8d29ce	
KB3115248 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4cc02a6f-9551-4909-bce1-4a45d41404ec	
KB4022199 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3f3c71ef-c743-4824-8951-deb8cdabf2eb	
KB4022137 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9d64be86-d3f2-47a4-a9a3-f8ae05842ed3	
KB4018310 Microsoft PowerPoint 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4cc49d2c-fe7e-4a55-987e-4b1d4ccb8e1c	
KB4011186 Microsoft Publisher 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4564150c-2ab1-42e4-a135-105b924dc45d	
KB4022202 Microsoft Word 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=59253783-a245-4897-993e-57a2ed30c0e0	
KB4011674 Microsoft Word 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b13107b6-02b9-4f00-a6d9-3bf44a3c1247	

KB4022141 Microsoft Word 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d2f428f2-7c02-4a49-8680-4407404cb7a2	
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

Windows 2008R2 (INW Server)

KB	Link	Notes
	Make the following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
HPESBHF03874 rev.1 ML350 Gen9 (CP035797)	https://support.hpe.com/hpsc/swd/public/detail?sp4ts.oid=1009483731&swItemId=MTX_2fad1bbda82e4d5ca0673a1b43&swEnvOid=4184	**Refer to ML350 Gen9 BIOS Update to 5/21/2018 Instructions above**
	Reboot Required	
KB4284826 June 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=999fa80e-c59d-4ff6-8268-c6a8c365f428	
	Reboot Required	

KB4338818 July 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1c930eab-7b7e-4616-b5b5-d6e4a723bc71	
	Reboot Required	
KB4338821	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8e951203-5d8e-4f69-9560-ce698c4f7a77	
	Reboot Required	
KB4343900 August 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=71600c77-2a56-4ba2-991b-ad477cfc9eb9	**Create the following registry settings if they do not exist** **Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]** **Value Name=[FeatureSettingsOverride]** **Type=[REG_DWORD]** **Data=[0]** **Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]** **Value Name=[FeatureSettingsOverrideMask]** **Type=[REG_DWORD]** **Data=[3]**
	Reboot Required	
KB4343894 IE 11	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6525d333-fafc-4345-ad06-6edc8db84aaf	
	Reboot Required	

KB4457144 September 2018 Monthly Rollup	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2986185e-cd31-4f1d-99a5-bea6bd1ef53c	
	Reboot Required	
KB4345590 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=14afae30-094f-4dca-ba5f-e22347edb98f	**Install KB4344149 first (restart if prompted) followed by KB4344152**
	Make the Following Registry Change	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reboot Required	

MLCL v6.9.6 Optional Security Updates

The following optional updates may be applied to further enhance the security profile of the MLCL systems. These updates should be evaluated on a site-by-site basis in accordance with local IT policy. The configuration changes in this section are compatible with MLCL product functionality but may introduce site specific IT impact as a result of disabling of legacy SSL protocols, prohibiting remote desktop usage and requiring certificate generation and maintenance.

Additional Security Setting and Patches

	INW Server	Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab	GE Client Review Workstation	Virtual Review
Patch	Download URL	Download URL	Download URL	Download URL
MS16-047 KB3149090 **Superseded**	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047

	INW Server	Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab	GE Client Review Workstation	Virtual Review
Plugin 20007 – Disable SSL V2/V3 – KB187498	Please see section - How to Install Plugin 20007 – Disable SSL V2/V3 – KB187498	Please see section - How to Install Plugin 20007 – Disable SSL V2/V3 – KB187498	Please see section - How to Install Plugin 20007 – Disable SSL V2/V3 – KB187498	Please see section - How to Install Plugin 20007 – Disable SSL V2/V3 – KB187498
Plugin 78479 - Poodle	No change needed. Step above fixes this.	No change needed. Step above fixes this.	No change needed. Step above fixes this.	No change needed. Step above fixes this.
Plugin 35291 – Weak Hashing	Please see section - How to Install Plugin 35291 – Weak Hashing (Refer to https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx for more information)	Please see section - How to Install Plugin 35291 – Weak Hashing (Refer to https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx for more information)	Please see section - How to Install Plugin 35291 – Weak Hashing (Refer to https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx for more information)	Please see section - How to Install Plugin 35291 – Weak Hashing (Refer to https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx for more information)
Plugin 45411	No change needed. Step above fixes this.	No change needed. Step above fixes this.	No change needed. Step above fixes this.	No change needed. Step above fixes this.
Plugin 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Please see section - How to Install Plugin 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Please see section - How to Install Plugin 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Please see section - How to Install Plugin 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Please see section - How to Install Plugin 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Plugin 63155 - Microsoft Windows Unquoted Service Path Enumeration	Please see section - How Remove Vulnerability for Plugin 63155 – Microsoft Windows Unquoted Service Path Enumeration	Please see section - How Remove Vulnerability for Plugin 63155 – Microsoft Windows Unquoted Service Path Enumeration	Please see section - How Remove Vulnerability for Plugin 63155 – Microsoft Windows Unquoted Service Path Enumeration	Please see section - How Remove Vulnerability for Plugin 63155 – Microsoft Windows Unquoted Service Path Enumeration
Plugin 59915 – Vulnerabilities in Gadgets Could	N/A	Please follow the section titled **"Disable the Sidebar in the system Registry"** in the following Article:	Please follow the section titled **"Disable the Sidebar in the system Registry"** in the following Article:	Please follow the section titled **"Disable the Sidebar in the system Registry"** in the following Article: https://technet.microsoft.com/library/s

	INW Server	Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab	GE Client Review Workstation	Virtual Review
Allow Remote Code Execution		https://technet.microsoft.com/library/security/2719662	https://technet.microsoft.com/library/security/2719662	ecurity/2719662
Disable SMB1 Protocol	Please see section How to Disable the SMB1 Protocol	Please see section How to Disable the SMB1 Protocol	Please see section How to Disable the SMB1 Protocol	Please see section How to Disable the SMB1 Protocol

Password Policy

Password Policy: Minimum Password Length may be changed above the 14 characters limit to meet security requirements. Refer to **Password** section of the Security Guide for further details about changing passwords.

Optionally Remove Abode Reader on INW Server

We recommend that abode reader be uninstalled on the INW Server. On the server Adobe reader is only used to review INW operator manual. The manual is available in printed format and through online manual portal.

Further MLCL Systems Security Recommendations

We strongly recommend following these recommendations:
- Change default password to stronger, more secure and unique for each user account
- Disable RDP in for each system using the following steps:
    - My Computer>Properties>Remote settings>Remote
    - Check "Don't allow connections to this computer".
    - Click ok and reboot.

- If Insite functionality is not used on the system then turn off the VNC service using the following steps:
    - Click on Start button
    - Click on Control Panel
    - Click on Administrative Tools
    - Double click Services
    - Right Click TightVNC Server and select Properties
    - Under Startup type select Disabled from the dropdown
    - Click on Apply and Ok

We also recommend following these general recommendations and the recommendations listed in MLCL Security guide
- Enhanced physical security
- Network firewalls
- Demilitarized Zones and perimeter defenses for site network
- Intrusion detection systems - network intrusion protection system
- Virtual Private Networks
- Network traffic analysis
- Log analysis

Contact Information

If you have any additional questions, please contact our Technical Support Department.