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 2 |
| **Subject:** | Security Information |
| **Date:** | 29 June 2018 |

## 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.

GE Healthcare

# CONTENTS

# Revision History

| Revision | Date | Comments |
|---|---|---|
| 1.0 | 22 September 2017 | • 6.9.6 document separation<br>• Qualified KB4025341 - July Monthly Rollup<br>• Added 6.9.6 Installation paths for simplifying patches installation<br>• 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 | 31 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<br>• Added missing qualified patches for virtual review<br>• Qualified minimum password length changes<br>• Changed verbiage from "Patch Refresh" to "Patch Updates"<br>• Further MLCL System Security Recommendations |

| 9.0 | 20 April 2018 | • Added January, February, March and April Qualified Patches<br>• 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<br>• Added Unqualified April Patch |
| 11.0 | 17 May 2018 | • Added May Qualified Patches<br>• Added .NET patches for versions 3.5 SP1, 4.5.2<br>• Added Microsoft Office Patches |
| 12.0 | 29 June 2018 | • Added Unqualified June Patch |

# 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 6.9.6R2 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 2**.
4. Click *Close*.
5. Close the application.

**Recommendation:** Use Internet Explorer (IE) for Catalog download. **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

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.

## 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.

GE Healthcare

- 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 2*, 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

GE Healthcare/29 June 2018

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.

## 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.

## OPTIONAL – How to Install INW Server Performance Enhancement

# GE Healthcare

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

**GE Healthcare**

# 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 chose 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 R2 Apply the updates from the following sections
    (i) MLCL v6.9.6 R2
    (ii) MLCL V6.9.6 2017 Patch Updates 1
    (iii) MLCL V6.9.6 2017 Patch Updates 2

(2) The machine was setup and initially patched but no subsequent updates have been applied.
  (a) For R2 Apply the updates from the following sections
    (i) Verify that all patches from section **MLCL v6.9.6 R2** have been applied. Install any unapplied patches
    (ii) MLCL V6.9.6 2017 Patch Updates 1
    (iii) MLCL V6.9.6 2017 Patch Updates 2

(3) The machine was setup and all previous patches have been applied
  (a) For R2 Apply the updates from the following sections
    (i) MLCL V6.9.6 2017 Patch Updates 2

## Unqualified Patches MLCL v6.9.6 R2

|  | 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 | HPSBHF03576 rev. 1<br>KB4284867 (CVE-2018-8225) | HPESBHF03805 rev.10<br>HPSBHF03576 rev. 1<br>KB4284867 (CVE-2018-8225) | HPESBHF03805 rev.10<br>HPSBHF03576 rev. 1<br>KB4284867 (CVE-2018-8225) | HPESBHF03805 rev.10<br>HPSBHF03576 rev. 1<br>KB4284867 (CVE-2018-8225) |

**MLCL V6.9.6R2**

| | 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 |
| Patch | Download URL | Download URL | Download URL | Download URL |
| | | | | |
| MS15-127 KB3100465 (Domain Controller only) | https://www.microsoft.com/en-us/download/details.aspx?id=50127 | N/A | N/A | N/A |
| MS15-067 KB3069762 | N/A | https://www.microsoft.com/en-us/download/details.aspx?id=47833 | https://www.microsoft.com/en-us/download/details.aspx?id=47833 | https://www.microsoft.com/en-us/download/details.aspx?id=47833 |
| HP System Management Homepage HPSBMU03380 Version: 7.5.4.3(1 Apr 2016) <mark>Superseded</mark> | https://h20566.www2.hpe.com/hpsc/swd/public/detail?idx=&action=driverDocument&itemLocale=&swItemId=MTX_544617581c264c8eaafe6b273a&mode<br><br>Please see section - How to Install HP System Management Homepage Patch on the INW Server – HPSBMU03380<br><br>**NOTE:** HPSBMU03051 must be installed before HPSBMU03380. | N/A | N/A | N/A |
| OPTIONAL – INW Server Performance Enhancement | Please see section – OPTIONAL - How to Install INW Server Performance Enhancement | N/A | N/A | N/A |

| | INW Server | Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab | GE Client Review Workstation | Virtual Review |
|---|---|---|---|---|
| Adobe Reader APSB15-15 <span style="background-color:red;color:white">Superseded</span> | ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.12/misc/ Download file - AdbeRdrUpd11012_MUI.msp<br><br>Please see section – How to Install Adobe Reader APSB15-15 | ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.12/misc/ Download file - AdbeRdrUpd11012_MUI.msp<br><br>Please see section – How to Install Adobe Reader APSB15-15 | ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.12/misc/ Download file - AdbeRdrUpd11012_MUI.msp<br><br>Please see section – How to Install Adobe Reader APSB15-15 | ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.12/misc/ Download file - AdbeRdrUpd11012_MUI.msp<br><br>Please see section – How to Install Adobe Reader APSB15-15 |
| MS11-025 KB2538242 | https://www.microsoft.com/en-us/download/details.aspx?id=26347 | | | |
| MS11-049 KB2251487 | https://www.microsoft.com/en-us/download/details.aspx?id=26419 | https://www.microsoft.com/en-us/download/details.aspx?id=26419 | https://www.microsoft.com/en-us/download/details.aspx?id=26419 | https://www.microsoft.com/en-us/download/details.aspx?id=26419 |
| MS13-081 KB2862330 | | | | https://www.microsoft.com/en-us/download/details.aspx?id=40507 |
| MS14-031 KB2957189 | | | | https://www.microsoft.com/en-us/download/details.aspx?id=43147 |
| MS14-066 KB2992611 | | | | https://www.microsoft.com/en-us/download/details.aspx?id=44633 |
| MS15-034 KB3042553 | https://www.microsoft.com/en-us/download/details.aspx?id=46480 | https://www.microsoft.com/en-us/download/details.aspx?id=46501 | https://www.microsoft.com/en-us/download/details.aspx?id=46501 | https://www.microsoft.com/en-us/download/details.aspx?id=46501 |
| | <span style="background-color:red;color:white">**Reboot Required**</span> | | | |

# MLCL V6.9.6 2017 Patch Updates 1

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

**GE Healthcare**

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.

| 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; Verify that .Net 4.5.2 shows in Control Panel\Programs and Features |
| Subsequent patches depend on installation of KB2901907. | | |
| KB2979596 | https://www.microsoft.com/en-us/download/details.aspx?id=44278 | Run from cmd prompt with SQLServer2008SP4-KB2979596-x86-ENU.exe /ACTION=Patch /INSTANCENAME=MSSQLSERVER /IGNORESERVICERESTARTSTATE |
| KB3020369 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f00e3c36-f5e3-465c-95d2-a84a22425868 | |
| KB3138612 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0bae11c4-626f-4b7e-b539-06c95cb014d5 | |

| | | |
|---|---|---|
| KB2639308 | https://www.microsoft.com/en-us/download/details.aspx?id=28929 | Install only .MSU file |
| IE11 | http://download.microsoft.com/download/9/2/F/92FC119C-3BCD-476C-B425-038A39625558/IE11-Windows6.1-x86-en-us.exe | Right click and Run as Administrator. If installation fail with a message requesting to connect to Internet, then install from the command line with these parameter /quiet /closeprogra<br>ms e.g. "IE11-Windows6.1-x86-en-us.exe /quiet /closeprograms"<br>Note: It could take few retry attempts to install. |
| **Reboot Required** | | |
| KB3125574 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7ed4c8c3-0f06-4227-99e3-e9f143394687 | |
| **Reboot Required** | | |
| KB3172605 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8382aa41-9de1-4bb2-b8b0-4ab89451be64 | |
| Adobe 11.0.19 **Superseded** | http://supportdownloads.adobe.com/detail.jsp?ftpID=6123 | |
| KB3179573 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fb159d73-16f1-4c8a-bc3a-c768f6e2a7ce | |
| KB4022719 **Superseded** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b9815359-6aad-467e-8666-2351fadc3c45 | |
| KB4012215 **Superseded** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=975bd6c2-d69f-48f9-bab5-b701e4a44294 | |

GE Healthcare

| KB3205402 <span style="color:red">**Superseded**</span> | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f8938e57-3bdd-411e-8bdd-38ebbac1db50 | Right Click and Run as Administrator; Apply KB3210139 and KB3210131 Only |
|---|---|---|
| <span style="color:red">**Reboot Required**</span> | - | |
| **Patches below can be applied in any order** | - | |
| kb947318 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ceff8ca0-08db-41d0-b825-fcc2cebaf8b4 | Do not run on Review Systems |
| KB3192391 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bc4fc430-38b5-4ef5-ba85-fb8254ac9be9 | |
| KB2538242 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bb49cc19-8847-4986-aa93-5e905421e55a | Install File with x86 in title |
| KB2538243 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=729a0dcb-df9e-4d02-b603-ed1aee074428 | Install 2 files with x86 in title; Select Repair option if required |
| KB2565063 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=719584bc-2208-4bc9-a650-d3d6347eb32e | Install 2 files with x86 in title; Select Repair option if required |
| KB2863902 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=73ab9cea-fa20-4d92-9719-f01f13f613c1 | |
| KB2863926 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=df24debf-341b-403b-9e0a-6cd01a025d8d | |
| KB2920748 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7ac78292-3a54-4100-837e-140fa85bb0bc | |
| KB2863817 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d0ab24c4-9edf-4faa-a69b-078470f6fd40 | Use all-convintl-en-us_......cab |

| | | |
|---|---|---|
| KB3104002 **Superseded** | https://www.microsoft.com/en-us/download/details.aspx?id=50346 | |
| KB3085528 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d7ba6a6e-7884-4042-a2ce-f236c43a0989 | |
| KB2881029 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3b158fbc-892b-4d1b-8c02-91682088ad72 | |
| kb2553432 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9badf612-4854-4023-9867-76e3677311af | |
| kb3118390 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4ecc22c5-46d4-40b2-a640-60e9da447657 | |
| kb3118378 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ae54ce3d-e321-4831-a1ba-fcae8eb430a0 | |
| kb3127953 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=95499009-678d-4bc4-96d9-384781a18627 | |
| KB3161949 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=25c0fd19-d4e4-4af5-aad9-f308dde496d5 | |
| KB2900986 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=82b62134-bafb-4fd3-815e-73534b9d1aa5 | |
| kb2850016 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3188a7d3-91d0-4780-897f-1990c4b3e952 | |
| KB3031432 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2ca8e6e8-fc4a-4974-a208-18cdf1d01d86 | Apply kb3004375 and KB3031432 |
| KB3059317 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9202ee09-24c9-4ae7-83bd-3b5d4b0e5c22 | |
| kb3101521 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=52d30a1b-2f14-4463-9034-92f46b76576d | |

| | | |
|---|---|---|
| kb2965313 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=a4474e45-3c37-4708-9a5a-31e3538ddd44 | Use all-wordintl-en-us_……cab |
| KB3156016 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f21d3be8-dd35-4ac7-97b8-b4d06d4ed7f2 | |
| KB3156019 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b5b7f2e4-bf3f-4974-ab23-f3a2ab886d31 | |
| KB3156017 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3f6acb0e-47be-458e-8559-ab9f1179dfba | |
| KB3159398 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2329e2b7-4e31-42e3-86aa-2ebfaa2c6339 | |
| KB3161958 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0fda0cfc-7ca1-4f78-ae19-90977c948ed3 | |
| KB3170455 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=65b4f1cb-3cd4-4546-8896-dc462d484282 | |
| KB3177186 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=88aaa062-4a7b-4690-ac06-8527d3db830d | |
| 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" |
| KB2880971 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fe594d9e-9828-451f-aa56-2c2cf431ade3 | |
| KB2810073 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=20c03f3c-cf50-4469-9e6a-c4f74622a160 | Only Run .MSP file |
| KB3000483 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=dbd91e47-4238-4bbe-8c8b-87c2d02c57d2 | Only Run 2 .MSU files |
| KB3054845 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=cd3cb1c0-dd41-45d0-a60d-794470b83761 | |

| | | |
|---|---|---|
| kb3054848 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=79ebf15b-3343-41fb-bf88-9bd6b4253fc0 | |
| kb3054835 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bd726abf-fa50-489d-ab30-fa13ee3e0ba0 | |
| kb3054842 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fc804f6e-c557-47e0-9f5e-4373b286677d | |
| KB3055044 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=58454b4a-dd6b-4902-865b-c57ce21d3b91 | |
| KB2553313 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f26e1911-9cf6-4082-8349-456230bc04ec | |
| KB2598244 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=aaa34820-0955-45db-b5a6-3048bb56843f | |
| KB3055033 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ef6e2e39-225f-4cad-97bb-200d1fab3e53 | |
| KB2965310 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fbe46296-974f-4eaf-ba1f-3f57787e932b | |
| KB3055039 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d5db1fcb-f98a-4b2d-abbc-003327425628 | |
| kb3085560 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6f15ec3c-4e27-483d-baed-6e17fba8ffc7 | Use all-convintl-en-us_......cab |
| kb3085526 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1c9e7d92-d1df-4cc4-8906-ff2429479d19 | |
| kb3101544 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5dddb0e6-6f66-4ae0-86e3-6a8d3d23a201 | |
| kb3101543 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=396a0e18-01af-4f19-a5ea-c5c9e352321f | |
| kb3085594 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=74ccaa37-b9c6-4c4c-a65b-da83e3e6341a | |

| kb | URL | Notes |
|---|---|---|
| kb2817478 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b1bbd02b-d4c3-48c3-b648-1852de5d2c8e | |
| kb3101520 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1e5f0476-1148-43b8-bfc4-10a1a29ddc32 | |
| kb3054984 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=35c6b5dc-c065-4d9a-a71f-9d0a6beb4df9 | |
| kb3115123 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e8bd0027-368c-4ecf-bc9b-5c64195e2c53 | |
| kb3114400 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=98015a12-b9cd-48ab-bd7f-7dea92bb8f67 | Use all-convintl-en-us_......cab |
| kb3114869 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7efaa3ba-dee4-45ba-84b0-50c7aa10437b | |
| kb3114885 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4ca07bc3-8c95-4644-be17-040a3964a02a | use all-onenoteint-en-us_....cab |
| kb3115474 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8bc2bfec-84bb-488e-ae91-f4814d409dba | use all-outlookintl-en-us_.....cab |
| kb3115471 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fd8a17d9-dad0-4f8d-95c4-0677ca0fbb08 | |
| kb3118309 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fb00cc28-9cb3-437e-bac5-069bc32f8aeb | |
| kb3128037 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=46311afb-a6ab-4fad-b6aa-4ec97507beba | |
| kb3118380 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=84ea23ce-49d8-4684-ac3b-45f0396053cf | |
| kb3114395 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=df66c1c1-7fab-4a43-886c-5203d1495bd8 | |
| kb2889841 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bb220b30-6d01-4e57-8db6-3e492d6b65d3 | |

| KB | Link | Notes |
|---|---|---|
| kb3128034 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9cd72446-5c11-433a-9589-fd85afcc4eb0 | |
| KB3178687 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=726adfc6-4ac9-4409-bdab-2892b7058e78 | |
| **Reboot Required** | | |
| KB3045311 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2fd51fbf-3f70-4c85-986b-5653b0fb7f11 | Only run x86 file; Run from a cmd prompt as Administrator using the following command: AMD64_X86-all-sqlserver2008-kb3045311-x86_30561aef89c6d174fee7b77bed6b3b8539542558.exe /ACTION=Patch /INSTANCENAME=MSSQLSERVER /IGNORESERVICERESTARTSTATE |
| **Reboot Required** | | |
| | 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 | |
| KB3138612 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5ae1092c-f211-4873-aabd-9ee1a142acbb | |
| KB2639308 | http://www.microsoft.com/en-ph/download/details.aspx?id=28933 | Install only .MSU file |
| IE11 | http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe | Right click and Run as Administrator. If installation fail with a message requesting to connect to Internet, then install from the command line with these parameter /quiet /closeprograms e.g. "IE11-Windows6.1-x64-en-us.exe /quiet /closeprograms" Note: It could take few retry attempts to install. |
| **Reboot Required** | | |
| kb3125574 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6147e6c1-663b-41bc-9582-9579343857d9 | |
| **Reboot Required** | | |
| Adobe 11.0.19 **Superseded** | http://supportdownloads.adobe.com/detail.jsp?ftpID=6123 | |
| KB3172605 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3363f98b-78a3-44a7-93df-d770b2dd150a | |
| KB3179573 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=366304fa-105b-4f48-a07e-d2e6bb274533 | |

| | | |
|---|---|---|
| KB4012215 **Superseded** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1f68a778-6adb-4ef6-948f-8f2ccdfff884 | |
| **Reboot Required** | | |
| **Patches below can be applied in any order** | | |
| kb2894844 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=00e0ded8-dc85-4017-8b54-a1456c63a61b | |
| KB3205402 **Superseded** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5036bd76-3251-49ba-ad86-a99b00853ad4 | Only apply KB3210139 (Right click and run as Administrator) & KB3210131 |
| KB2972216 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e63b4eca-27a1-4fd0-b311-e468da0cd02e | |
| KB2972107 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=151e15f7-fa7a-40c4-a58a-721cb88e8071 | |
| KB2979578 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d44bd7d1-ec33-4a65-942c-093aec39b02b | |
| KB2978128 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e257d135-40b9-4361-9e7d-8537d256d54b | |
| KB3074230 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d0baf87d-e8ec-4ddc-b8b0-89f668ee6504 | |
| KB3074550 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2f7719fa-8a6d-4b16-9c69-66447f308ee7 | |
| KB3097996 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=103a0bdd-e71c-4f33-8cf1-7b68198ad536 | |

| | | |
|---|---|---|
| KB3098781 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4ed6e065-7e37-44bb-8798-245649851dec | |
| KB3122656 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=428c2fef-afe5-46a7-a454-da2fa0e3af27 | |
| KB3127229 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8f49f137-0741-498e-9f7c-754862054221 | |
| KB3135996 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=24aeb988-b368-435b-923b-c09b8a2d3fa5 | |
| KB3142033 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=eac1599f-2887-40ce-9cf4-0f364dc37343 | |
| KB3159398 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=56a7a134-5ad6-43c2-aab1-e10d2fef8f7c | |
| KB3161949 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5bc0e07b-33ca-4ea2-8253-4f0dcd26783a | |
| KB3170455 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=45460055-be25-47ad-ad0a-2a4711fcca74 | |
| KB3163251 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7b053e5b-04a5-4f47-92c5-74f6caba0de7 | |
| KB3125869 | https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015 | |
| KB2538243 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=729a0dcb-df9e-4d02-b603-ed1aee074428 | Only run X86-all-vcredist_x86…. |
| KB3156016 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=de32fc3d-60a4-4fc9-9588-0c404765940a | |
| KB3156019 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=05cb4345-49ea-4eca-8ba3-f870466c46c7 | |
| KB3161958 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=795571cf-bd8d-4602-bb28-11080e614333 | |

| | | |
|---|---|---|
| HPSBMU03653 rev.1 | https://h20566.www2.hpe.com/hpsc/swd/public/detail?swItemId=MTX_083799d6dad34195bb47cb43c1 | |
| **Reboot Required** | | |
| KB3045311 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2fd51fbf-3f70-4c85-986b-5653b0fb7f11 | Only run x64 file; Run from a cmd prompt as Administrator using the following command: AMD64-all-sqlserver2008-kb3045311-x64_37a197c60990d2e83e98d1090109a4ab3f2abe4b.exe /ACTION=Patch /INSTANCENAME=MSSQLSERVER /IGNORESERVICERESTARTSTATE |
| **Reboot Required** | | |
| | Make the following Registry Change | |
| | **[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]** | |
| | **State=dword:00010000** | |

## 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.

**GE Healthcare**

## 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 11.0.20 | http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191 | |
| 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 | |
| KB3213624 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3658f96e-a521-429d-a9a9-e70e30f5d830 | |
| KB4025341 July Rollup 2017 | https://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=12c93ad9-ef0e-4ce6-8a1d-84713223d24a | |

| 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, |
|---|---|---|
| **Reboot Required** | | |
| 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 | |
| HPSBHF03557 Rev. 1 | ftp://ftp.hp.com/pub/softpaq/sp80001-80500/sp80050.exe | Apply only to 6.9.6 R2 system. Not applicable for Virtual Review. |
| HP z440 BIOS Update | https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828 | |
| | **Make the Following Registry Change** | |
| | **[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]** | |
| | **State=dword:00010000** | |
| 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** | |
| **Windows 2008R2 (INW)** | | |

| | | |
|---|---|---|
| | 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 | |
| KB4025341 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b2423c5b-0254-4747-88bb-ec1a785549cb | |
| 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,** |
| **Superseded** KB4034664 August Rollup 2017 | https://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=80f7899d-451d-4e3f-b54e-d488a06a3c58 | To successfully install this Rollup, you must uninstall July Rollup **KB4025341 and reboot before installing KB4034664** |
| | **Make the following Registry Change** | |
| | **[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]**<br><br>**State=dword:00010000** | |
| | **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters]**<br><br>**LdapEnforceChannelBinding=DWORD:1** | Apply only on Domain Controller. Need starting July Rollup-KB4025341 (CVE-2017-8563) |

## MLCL V6.9.6 2017 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) 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**<br><br>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<br><br>**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]<br><br>State=dword:00010000 | |

GE Healthcare

## 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.

Refer to the above links for the following previously qualified patches KB2862330, KB2957189, KB2992611, KB4022719, KB2979596 and KB3045311.

   **NOTE: KB2979596 should be applied first before KB3045311**

These patches were previously qualified but not listed. Please apply these patch to the virtual review system other systems do not require these patches to be installed separately. In case you receive a message like "**Not applicable to the computer**" ignore, that is an indication that the patch already exist on the system.

## 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 July 2017 Microsoft Office 2010 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a | |
| KB3213626 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2bb1487f-b287-41a9-b0ec-01b42aa4759e | |

---

**GE Healthcare**

| | | |
|---|---|---|
| **September 2017 Microsoft Office 2010** | | |
| **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 January 2018 Microsoft Excel 2010** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d7594745-04d5-4631-b2d7-289816f4dd43 | |
| **KB4011659** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0b5a1bf0-3043-47fd-afc3-d2fb55a46a96 | |

| | | |
|---|---|---|
| **January 2018 Microsoft Word 2010** | | |
| **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 December 2017 Monthly Rollup | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=09064e30-6f3e-4c99-8d09-fbc2ba06b436 | |
| | **Reboot Required** | |
| KB4054172 | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fdecaf44-50a3-4667-a935-f9e7af0bb317 | |

| January 2018 .NET Framework | | |
|---|---|---|
| **KB2269637** | Create the following Registry Keys | |
| | **Key=[ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\]** <br> **Value Name=[CWDIllegalInDllSearch]** <br> **Type=[REG_DWORD]** <br> **Data=[1]** | |
| | Make the Following Registry Change | |
| | **[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]** | |
| | **State=dword:00010000** | |
| | <u>**Reboot Required**</u> | |
| | | |

## 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:

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)**<br>2) **KB4095874**<br>3) **KB4096495** |
| | <span style="color:red">**Reboot Required**</span> | |
| **KB4022146**<br>**Microsoft Excel 2010** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5795d737-4091-4784-a707-007b99d3daef | **KB4022146**<br>**Microsoft Excel 2010** |
| **KB2899590**<br>**Microsoft Office 2010** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d8acdbaf-7f56-4c65-a898-9fdfc7a2d83a | **KB2899590**<br>**Microsoft Office 2010** |
| | Make the Following Registry Change | |
| | **[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]** | |
| | **State=dword:00010000** | |
| | <span style="color:red">**Reboot Required**</span> | |

## 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** |
| | <span style="color:red">**Reboot Required**</span> | |
| **KB4056894 January 2018 Monthly Rollup** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fc887fd2-cd35-434b-b6e3-1fef99b2e7ce | |
| | <span style="color:red">**Reboot Required**</span> | |
| **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 | |
| | <span style="color:red">**Reboot Required**</span> | |
| **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 | |
| **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 | |
| | <span style="color:white">**Reboot Required**</span> | |
| **KB4093118 April Monthly Rollup** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d2c7363c-323f-4e92-892a-90b83027e4aa | |
| | <span style="color:white">**Reboot Required**</span> | |
| **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 |
| | <span style="color:white">**Reboot Required**</span> | |
| **KB4103718 May 2018 Monthly Rollup** | http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4fe75106-a2ba-4186-aecd-10424a19225e | |
| | <span style="color:white">**Reboot Required**</span> | |
| **KB4095874 .NET 3.5 SP1 and KB4096495 .NET 4.5.2** | 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 patch for KB4095874 and KB4096495. The downloaded** |

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

## 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<br>KB3149090 | 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 |

# GE Healthcare

| | 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** | 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: |

**GE Healthcare**

| | INW Server | Acquisition - Mac-Lab IT/XT/XTi , CardioLab IT/XT/XTi and SpecialsLab | GE Client Review Workstation | Virtual Review |
|---|---|---|---|---|
| Could Allow Remote Code Execution | | https://technet.microsoft.com/library/security/2719662 | https://technet.microsoft.com/library/security/2719662 | https://technet.microsoft.com/library/security/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.