Invasive Cardiology Security Website

Interventional - Invasive Cardiology

Product Group:	Interventional Invasive Products
Products:	Mac-Lab, CardioLab and ComboLab Recording Systems, Centricity Cardiology Data Management Systems
Version:	AltiX (v7)
Subject:	Security Information
Date:	02 March 2020

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 and CardioLab 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, CardioLab, GE Acquisition/Client Review and INW Server hardware/software.
- If a vulnerability meets Mac-Lab and CardioLab 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 and CardioLab vulnerability, the GEHC Product Security Database and Invasive Cardiology Security Website and affected Mac-Lab and CardioLab Security Patch Installation Instructions are updated.

The Mac-Lab and CardioLab vulnerability validation criteria are as follows: Any vulnerability that allows malware to alter or deny Mac-Lab and CardioLab 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 and CardioLab impact. Once a security patch is validated, customers are responsible for the installation of security patches. All Mac-Lab and CardioLab Security Patch Installation Instructions are available on the Invasive Cardiology Security Website.

Vulnerabilities exposed after the Mac-Lab and CardioLab 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 , CardioLab and Centricity INW systems and will not be validated.

CONTENTS

Revision History

Revision	Date	Comments
1.0	05 November 2019	• Listed Qualified August 2019 Patches • Listed Qualified September 2019 Patches • Listed Service Stack Update Patch for server
2.0	02 December 2019	• Listed Qualified October 2019 Patches
3.0	09 December 2019	• Listed Qualified November 2019 Patches
4.0	06 January 2020	• Listed Service Stack Update Patch • Listed Qualified December 2019 Patches
5.0	20 January 2020	• Listed Qualified January 2020 Patches
6.0	02 March 2020	• Listed Qualified February 2020 Patches

Document layout

The document is structured to show

- Requirements for installation of patches
- How to confirm the version of AltiX application.
- How to logon to the system
- Subsections that are referenced from patch update sections
- Unqualified patches
- Patch update sections

Installation of the Security Patches on MLCL systems

Requirements:

- Updates may be applied at any time other than while the Mac-Lab or CardioLab 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 provides list of qualified patches for INW Server (Windows Server 2016), Acquisition (Windows 10) and Review (Windows 10) systems.

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

1. Launch the Mac-Lab CardioLab application from the acquisition or review system.
2. Select ***Help > About Mac-Lab*** (or ***CardioLab***, as applicable).
3. Verify the version number is **7.0.0**
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/Review/INW Server Systems

Login as user who has administrative privilege to deploy the security patches.

NOTE: For initial install MLCLTechUser account can be used and for follow up account contact the site for appropriate account information.

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.

It is the responsibility of the Hospital to assure all the qualified patches have been installed on the systems.

Unqualified Patches MLCL v7.0.0

	INW Server	**Acquisition**	**GE Client Review Workstation**
Operating System Platform	**Windows Server 2016**	**Windows 10**	**Windows 10**
Current Unqualified Vulnerability	**KB4505225**	**KB4505225, DSA-2019-072**	**KB4505225, DSA-2019-072**

MLCL V7 2019 Patches

Note: During installation of patches, if message box appears requesting system restart. Kindly restart the system.

Windows 10 LTSB 1607 x64 (Acquisition & GE Review)

KB	Link	Notes (Applicable Patches. Patches to be applied in the order listed.)
KB4512517	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4512517	Windows 10 LTSB version 1607 x64 Cumulative Security Update 08-2019
KB4516044	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4516044	Windows 10 LTSB version 1607 x64 Cumulative Security Update 09-2019
KB4524152	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4524152	Windows 10 LTSB version 1607 x64 Cumulative Security Update for IE
KB4519998	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4519998	Windows 10 LTSB version 1607 x64 Cumulative Security Update 10-2019
KB4525236	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4525236	Windows 10 LTSB version 1607 x64 Cumulative Security Update 11-2019
KB4520724	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4520724	Windows 10 LTSB version 1607 x64 Service Stack Update 11-2019
KB4530689	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4530689	Windows 10 LTSB version 1607 x64 Cumulative Security Update 12-2019

KB4534271	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4534271	Windows 10 LTSB version 1607 x64 Cumulative Security Update 01-2020
KB4537764	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4537764	Windows 10 LTSB version 1607 x64 Cumulative Security Update 02-2020

Windows Server 2016 (INW)

Note: Customer can install applicable Microsoft SQL Server 2017 and Operating System security patches released prior to July 2019.

KB	Link	Notes (Applicable Patches. Patches to be applied in the order listed.)
KB4509091	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4509091	Service Stack Update 07-2019 for Windows Server 2016 x64-based Systems
KB4512517	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4512517	Cumulative Security Update 08-2019 for Windows Server 2016 x64-based Systems
KB4516044	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4516044	Cumulative Security Update 09-2019 for Windows Server 2016 x64-based Systems
KB4524152	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4524152	Cumulative Security Update for IE for Windows Server 2016 x64-based Systems
KB4519998	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4519998	Cumulative Security Update 10-2019 for Windows Server 2016 x64-based Systems
KB4525236	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4525236	Cumulative Security Update 11-2019 for Windows Server 2016 x64-based Systems

KB4520724	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4520724	Service Stack Update 11-2019 for Windows Server 2016 x64-based Systems
KB4530689	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4530689	Cumulative Security Update 12-2019 for Windows Server 2016 x64-based Systems
KB4534271	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4534271	Cumulative Security Update 01-2020 for Windows Server 2016 x64-based Systems
KB4537764	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4537764	Cumulative Security Update 02-2020 for Windows Server 2016 x64-based Systems
Software Only Review (Windows 10 Pro, Windows 10 Enterprise)		
Note: All applicable released patches are qualified, and it is the responsibility of hospital to keep them up to date.		

Contact Information

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