

Customer Technical Bulletin

CTB-00456

Date: 07/1	11/2018		
Author:	Service Engineering		
Product:	Referenced in Document	Subsystem:	Microsoft Windows OS
Subject:	Hologic Policy for Critical Mic	rosoft Windows C	perating System Patches

Purpose

To introduce Hologic's policy for releasing critical patches for our latest release of the Microsoft Windows Operating System.

Scope

Microsoft releases critical patches on a regular basis and Hologic is committed to ensuring the integrity of our customers' systems. Under this new policy, Hologic will closely monitor Microsoft's critical patching schedule and actively verify, validate and release these patches on a regular basis. This will typically be within 30 days of the patch release but may vary based on the complexity of the patch or the threat assessment of the vulnerability.

Once the patches are validated, Hologic will provide a list of patches for our customers via the Hologic.com support website (<u>https://www.hologic.com/package-inserts/breast-skeletal-health-products</u>) under CyberSecurity for each product. Links for each product can be found below.

Dimensions (AWS)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/selenia-dimensions-mammography-system-package
3Dimensions (AWS)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/3dimensions-mammography-system
Affirm Prone Biopsy System (AWS)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/affirm-prone-breast-biopsy-guidance-system-package
SecurView	https://www.hologic.com/package-inserts/breast-skeletal-health- products/securview-diagnostic-workstations-package
Cenova (Image Analytics)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/image-analytics-package-insertsifus
Trident	https://www.hologic.com/package-inserts/breast-skeletal-health- products/trident-specimen-radiography-system-package
Brevera	https://www.hologic.com/package-inserts/breast-skeletal-health- products/brevera-breast-biopsy-system

CTB-00456 Rev 002

Page 1 of 8

CSD-0044-T03 Rev 003

©2012 Hologic, Inc. The information contained in this document, including references to software and/or firmware, is considered proprietary, and is for sole use by Hologic Inc., its authorized sales and service agents and Hologic product owners. All other distribution is strictly prohibited.

Horizon (Apex/DXA/QDR)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/horizon-dxa-system-package-insertsifus
Discovery (Apex/DXA/QDR)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/discovery-dxa-system-package-insertsifus
Fluoroscan (Insight/InsightFD)	https://www.hologic.com/package-inserts/breast-skeletal-health- products/fluoroscan-mini-c-arm-package-insertsifus

Supported Products

The instructions provided in this document apply to the following products:

- Affirm Prone Biopsy System
- > Dimensions
- > 3Dimensions
- > Trident
- > Brevera
- SecurView
- Cenova
- Horizon (Apex/DXA/QDR)
- Discovery (Apex/DXA/QDR)
- Fluoroscan (Insight/InsightFD)

Obtaining the Microsoft Patch

Using the list of validated patches obtained from the links above, follow the below steps to download each patch:

NOTE: To obtain a list of patches that are already installed on your system, follow the confirming patch installation steps provided for each product later in this document. This list can be compared with the list of validated Hologic patches to determine what patches are needed for your specific system.

- 1. Navigate to the following link from your internet browser on a PC with an internet connection: <u>https://portal.msrc.microsoft.com/en-us/security-guidance</u>
- 2. Using the search on CVE number or KB Article search field, type the number (omitting the KB) of the KB. Once the results are displayed, select the patch for the applicable OS as shown below.

0 From 1	BV13/2017 To E 10/12/2017 All Product Categories	• Al Products • Al	Seventes	· Atlmpatt
* 4253	α * <i>ρ</i>			
telease I	Notes Number only			
Date 🔻	Release			
10/10/2017	October 2017 Security Updates			
ecurity	Updates ik 🗄 breety 🗒 brant	firtar ta	t to the when t	Down
Dete 🖤	Product	Pattern	Article	Devendsort
81/11/2017	Internet Explorer 11	Internet Explorer 11 Windows Server 2008 R2 for x64 faxed Systems Server Pack 1	4525345	Monthly Rollup
			4029292	Il Cumulative
17/11/2017	Internet Englisher 11	Windows 7 for x84-based Systems Service Pack 1	1 4025341	Monthly Rokup
			4025252	H Cumulative
1/11/2017	Internet Explorer 11	Windows 7 for 32-bit Systems Service Pack 1	+025341	Manthly Rolup
		#125252	31 Cumulative	
17/21/2017	Windows Server 2008 82 for e64-based Systems Service Pack 1		4025341	Martity Rollag
			4025337	Security Only
87/11/2017	Windows Server 2008 R2 for Sanium Based Systems Service Fack 1		4025341	Monthly Rolling
			4525337	Security Dily
17/11/2017	17 Wednes 7 for ef4-based Systems Service Pack 1 Patch Selection	Patch Selection -	4025341	Marchly Rohat
		#025337	Security Crity	

3. This will open the Microsoft Update Catalog page where you can select the download option for the applicable OS patch.

Microsoft Update Catalog			KB402	5341	Search	
Search results for "XB402S341"						
Updates: 1 - 6 of 6 (page 1 of 1)						Previous Next -;
Title	Products -	Classification	Last Updated	Version	Sav	
2017-07 Security Monthly Quality Rollup for Windows Server 2008 R2 for e64-based Systems (K34025341)	Windows Server 2008 R2	Security Updates	7/10/2017	ri/a	191.6 MB	Doenload
2017-07 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (R04025341)	Windows 7	Security Updates	7/10/2017	n/a		Download
2013 GT Security Ministry Could's Endue for Westness Server 2008 62 for Bansum Assed Systems (CBR025161)	Windows Server 2008 R2	Security Updates	7/10/2017	ri/a	100.4 MB	Download
2017-07 Security Munitity Quality Rollup for Windows Embedded Standard 7 for abli-based Systems (KE4025341)	Windows Embedded Standard 7	Security Updates	7/10/2017	n/a	117.1 M8	Download
2017-07 Security Ministry Quality Rolling for Windows Entended Standard 7 for All-Exectly Ministry Quality Rolling for Windows 7 for All-Exectly Systems (OR4025341) 2017-07 Security Ministry Quality Rolling for Windows 7 for All-Exectlystems (OR4025341)	Windows Embedded Standard 7 Windows 7	Security Updates Security Updates	7/10/2017 7/10/2017	n/a n/a	117.1 MB	Download Download

- D 2017 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | telp
- 4. Once downloaded, the patch can be installed

Installing the Patch

Installation of the patch requires administrator access to the system. Please reference your training material or contact Hologic Support to obtain login credentials.

Affirm Prone Biopsy System, Dimensions/3Dimensions, Trident, and Brevera products

- Perform the following steps to exit the application and access the Windows desktop: Note: For any questions or clarification with these steps, please reference the appropriate product User Manual.
 - a. Log out of the application.
 - b. Hold the **CTRL** key on the keyboard while clicking **Shutdown** in the application. This will take you to the Login/Exit screen. Hold the **CTRL** key on the keyboard while clicking **Exit** to exit the application and allow access to the Windows desktop.
- 2. Enable and start the Windows Update service:

Note: Please reference the links in the "Obtaining the Microsoft Patch" for your particular Windows Operating System.

- a. Press the Windows key on the keyboard to access the Start Menu.
- b. In the start menu search box, type **services.msc**.

CTB-00456 Rev 002

- c. Click on services.msc displayed in the list above.
- d. Find the Windows Update service in the list, right click on the service and select Properties from the menu that appears. If the service in enable and set to Automatic skip to step j.
- e. Set the Windows Update service startup type to Automatic.
- f. Click Apply.
- g. Click Start.
- h. Click **OK** to close the Windows Update service properties window.
- i. In the Services window, confirm that the Windows Update service now has a startup type of Automatic and that its status is Started.

Windows Update Enables the ... Started Automatic

- j. Close the Services window.
- 3. Once the patch has been placed on the Hologic system (via direct download or removable media), start the installation by double clicking on it.
- 4. Step through the installation dialogs that appear until the patch installation is completed.
- 5. At the Installation complete window, click **Restart Now** or perform a manual restart of the PC if not prompted.
- 6. The computer will restart.
- 7. If the Windows Update service was enabled in steps above, set it back to a disabled state:
 - a. Access the Windows desktop using instructions provided in earlier steps.
 - b. Press the Windows key on the keyboard to access the Start Menu.
 - c. In the start menu search box, type **services.msc**.
 - d. Click on services.msc displayed in the list above.
 - e. Find the **Windows Update** service in the list, right click on the service and select **Properties** from the menu that appears.
 - f. Set the Windows Update service startup type to **Disabled**.
 - g. Click Apply.
 - h. Click Stop.
 - i. Click **OK** to close the Windows Update service properties window.
 - j. In the Services window, confirm that the Windows Update service now has a startup type of Disabled.

🐫 Windows Update 🛛 Enables the ... 👘 🖉 Disabled

- k. Close the Services window.
- 8. Confirming Patch Installation
 - a. Login to Windows as administrator. Please see "*Installing the Patch*" above for login instructions for Hologic products.
 - b. Press the Windows key on the keyboard to access the Start Menu.
 - c. In the start menu search box, type **Programs and Features**.
 - d. Click on Programs and Features displayed in the list above.
 - e. In the Programs and Features window, click the View installed updates link.
 - f. Installed updates list is presented. Give it a couple minutes to load completely.
 - **g.** Confirm that the Microsoft Patch is listed as installed.

Note: You can sort the list by "Installed On" column to make it easier to see the

CTB-00456 Rev 002

patches that were just installed.

Fluoroscan (Insight/InsightFD) products

Note: Ensure you have archived all images and performed a system backup on the unit before proceeding.

- 1. Exit the InSight application by doing the following:
 - a. Click on the "System Configuration" menu item and select "Administrative Settings".
 - b. On the "System Configuration" dialog, select the "Administrative Settings" tab.
 - c. In the "System Shutdown" section, uncheck the "Shut down Fluoroscan upon application shutdown".
 - d. Press the "OK" button to apply the settings and close the dialog.
 - e. On the main menu, click on the "Exit" menu item and select "Exit".
 - f. This will display the Windows desktop.
 - g. Once the patch has been placed on the Hologic system (via direct download or removable media), start the installation by double clicking on it.
 - h. Step through the installation dialogs that appear until the patch installation is completed.
 - i. At the Installation complete window, click **Restart Now** or perform a manual restart of the PC if not prompted.
 - j. The computer will restart.
 - k. Wait for the Fluoroscan application to start.
 - I. After the computer restarts, confirm that the patch has been installed by performing the following:
 - i. Minimize the Fluoroscan application
 - 1. For Windows 7:
 - a. Click on the "Windows Start Button > Control Panel > Windows Update"
 - b. In the Windows Update Dialog, on the left menu bar, click "View Update History".
 - ii. Confirm the patch you installed is shown in the list
 - iii. Close all open dialog boxes.
 - iv. Maximize the Fluoroscan application

Discovery/Horizon (Apex/DXA/QDR)

Note: Ensure you have archived all images and performed a system backup on the unit before proceeding.

- 1. Shutdown the system by performing the following:
 - a. On the application desktop click on the "**Exit**" button which will bring up the "Exit System" dialog.
 - b. Select "Exit with shutdown" button and then click "OK".
 - c. The system will be powered off.
- 2. Restart the PC.
- 3. Log in as the **Admin**, only an Admin should perform the necessary patch update.
- 4. When the system boots into the Hologic Apex application, exit the Hologic Apex application by doing the following:
 - a. On the application desktop click on the "**Exit**" button which will bring up the "Exit System" dialog.
 - b. Select "Exit without shutdown" button and then click "OK".
 - c. This will display the Windows desktop
 - d. Once the patch has been placed on the Hologic system (via direct download or removable media), start the installation by double clicking on it.
 - e. Step through the installation dialogs that appear until the patch installation is completed.
 - f. At the Installation complete window, click **Restart Now** or perform a manual restart of the PC if not prompted.
 - g. The computer will restart.
 - h. Wait for the Apex application to start.
 - i. After the computer restarts, confirm that the patch has been installed by performing the following:
 - j. Minimize the Apex application
 - i. For Windows 7:
 - Click on the "Windows Start Button > Control Panel > Windows Update"
 - 2. In the Windows Update Dialog, on the left menu bar, click "View Update History".
 - ii. Confirm the patch you installed is shown in the list
 - iii. Close all open dialog boxes.
 - k. Maximize the Apex application

Customer Suggestions

- As with any network security program, vigilance is key to ensure internal systems are never compromised. Having a hardened, resilient network environment that is able to deal with security compromises is essential. Hologic is committed to monitoring these compromises and quickly working to resolve them. At the same time, Hologic recommends incorporating standard security practices that incorporate proactive security mechanisms that deal with emerging zero-day vulnerabilities and exploits.
- Check out the Hologic support web portal (<u>https://www.hologic.com/package-inserts/breast-skeletal-health-products</u>) for validated Antivirus software for each Hologic product. It's recommended that one of these packages be installed on our devices and updated with latest virus definitions.
- Avoid personal activities such as surfing the internet, downloading files, and checking email on Hologic medical devices.
- Block SMB traffic at your network perimeter whenever possible to limit exposure of unpatched devices to the internet and implement secure networking techniques, such as network segregation where appropriate.

Additional Resources

https://www.us-cert.gov/ncas/alerts/TA17-132A https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx http://www.hologic.com/support