HOLOGIC®

Customer Technical Bulletin

CTB-00456

Date: *June 4, 2020*

Author: Service Engineering

Product: Referenced in Document   **Subsystem:** Microsoft Windows OS

Subject: **Hologic Policy for Critical Microsoft Windows Operating 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 Cybersecurity landing page of the Hologic.com website (https://www.hologic.com/support/usa/breast-skeletal-products-cybersecurity).

Supported Products

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

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

Before using this document, please consult Agile for the latest revision.

Technical Bulletin (cont.)

Obtaining the Microsoft Patch

Using the list of validated patches obtained from the link 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: https://portal.msrc.microsoft.com/en-us/security-guidance

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.

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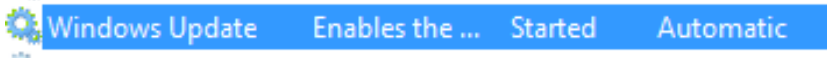

4. Once downloaded, the patch can be installed

Technical Bulletin (cont.)

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, Trident HD and Brevera products

1. 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**.
     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.

     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.
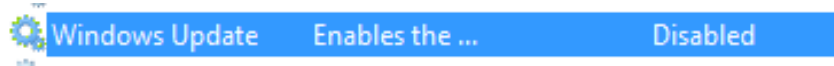
  k. Close the Services window.

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 **Control Panel**.

   i. If the search box isn't visible in Windows 10, just start typing.

  d. Click on Control Panel displayed in the list above.

  e. Double-click Programs and Features from the Control Panel menu.

  f. In the Programs and Features window, click the **View installed updates** link.

  g. Installed updates list is presented. Give it a couple minutes to load completely.

  h. 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 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.

Technical Bulletin (cont.)

    j.   The computer will restart.

    k.   Wait for the Fluoroscan application to start.

    l.   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**.

            2.   For Windows 10:

                a.   Click on the Windows Start Button and type **Control Panel**.

                b.   Click on **Control Panel** from the list of displayed search results.

                c.   Double-click **Programs and Features** from the Control Panel menu.

                d.   In the Programs and Features window, click the **View installed updates** link.

                e.   Installed updates list is presented. Give it a couple minutes to load completely.

                f.   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 patches that were just installed.

        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.

Note: For Windows 10 systems the Windows Update service must be enabled before installing any Windows Updates and disabled again after installing any applicable Windows Updates.

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
    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.
    2. For Windows 10:
        a. Click on the Windows Start Button and type Control Panel.
        b. Click on Control Panel from the list of displayed search results.
        c. Double-click Programs and Features from the Control Panel menu.
        d. In the Programs and Features window, click the View installed updates link.
        e. Installed updates list is presented. Give it a couple minutes to load completely.
        f. Confirm that the Microsoft Patch is listed as installed.
    3. **Note: You can sort the list by "Installed On" column to make it easier to see the patches that were just installed.**
k. Confirm the patch you installed is shown in the list
l. Close all open dialog boxes.
m. 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 can deal with security compromises is essential. Hologic is committed to monitoring these compromises and quickly working to resolve them. At the same time, Hologic

Technical Bulletin (cont.)

recommends incorporating standard security practices that incorporate proactive security mechanisms that deal with emerging zero-day vulnerabilities and exploits.

➢ Check out the Cybersecurity landing page on the Hologic.com website (https://www.hologic.com/support/usa/breast-skeletal-products-cybersecurity) for validated Antivirus software for each Hologic product. It is 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