

### CTB-01038

**Date:** 3/23/2022

**Author:** Service Engineering

**Product:** Hologic Connect™      **Subsystem:** N/A

**Subject:** PTC Axeda agent and Axeda Desktop Server Vulnerability Mitigation

---

#### **Purpose:**

Vulnerabilities in the Axeda agent environment have recently been discovered, and CISA (Cybersecurity & Infrastructure Security Agency) has published ICS Advisory (ICSA-22-067-01). More information on the advisory can be found here:

<https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01>.

Axeda is the IoT agent used by our Hologic Connect remote support platform. This Customer Technical Bulletin (CTB) is to provide our service and support teams, and our customers with recommended mitigation strategies for Hologic products that are likely to be running Hologic Connect.

#### **Scope:**

All currently supported Hologic product systems running Windows 7 or Windows 10 that have Hologic Connect installed, whether Hologic Connect is actively connected or not. Product systems in scope include, but are not limited to:

- 3Dimensions™ Mammography System
- Selenia® Dimensions® Mammography System
- Selenia® Full-Field Digital Mammography System
- SecurView® Workstations
- Cenova™ Image Analytics Server
- Affirm® Prone Biopsy System
- Brevera® Breast Biopsy System
- Trident® HD Specimen Radiography System
- Aegis® MultiView™ Software
- RosettaDC™ Tomosynthesis data converter
- Horizon® DXA System
- Discovery® DXA System
- Fluoriscan® InSight® Mini C-arm Extremities Imaging System
- Unifi™ Workspace
- Dicom 6000 software

#### **Important Note:**

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

# Technical Bulletin (cont.)

## Verifying Vulnerability:

If desired, check to see if the system is vulnerable before applying the mitigation.

1. Refer to “Exiting the Hologic application” later in this bulletin.
2. Open Services.msc from the Control Panel or by searching Services in the Start menu.
3. Confirm the following services are not present:
  - TightVNC Server
  - Hologic Connect
  - Axeda Desktop Server

## Exiting the Hologic application:

### **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. Refer to the Mitigation Procedure later in this bulletin.

### **Fluoroscan (Insight and InsightFD) products**

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

1. Perform the following steps to exit the InSight application and access the Windows desktop:  
*Note: For any questions or clarification with these steps, please reference the appropriate product User Manual.*
  - 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”.
2. Refer to the Mitigation Procedure later in this bulletin.

### **Discovery/Horizon (Apex/DXA/QDR)**

*Note: Ensure you have archived all images and performed a system backup on the unit before proceeding. For any questions or clarification with these steps, please reference the appropriate product User Manual.*

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.

## Technical Bulletin (cont.)

2. **Restart** the computer.
3. Log in as the **Admin**.
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**”.
5. Refer to the Mitigation Procedure later in this bulletin.

### All other products not specifically listed

*Note: For any questions or clarification with these steps, please reference the appropriate product User Manual.*

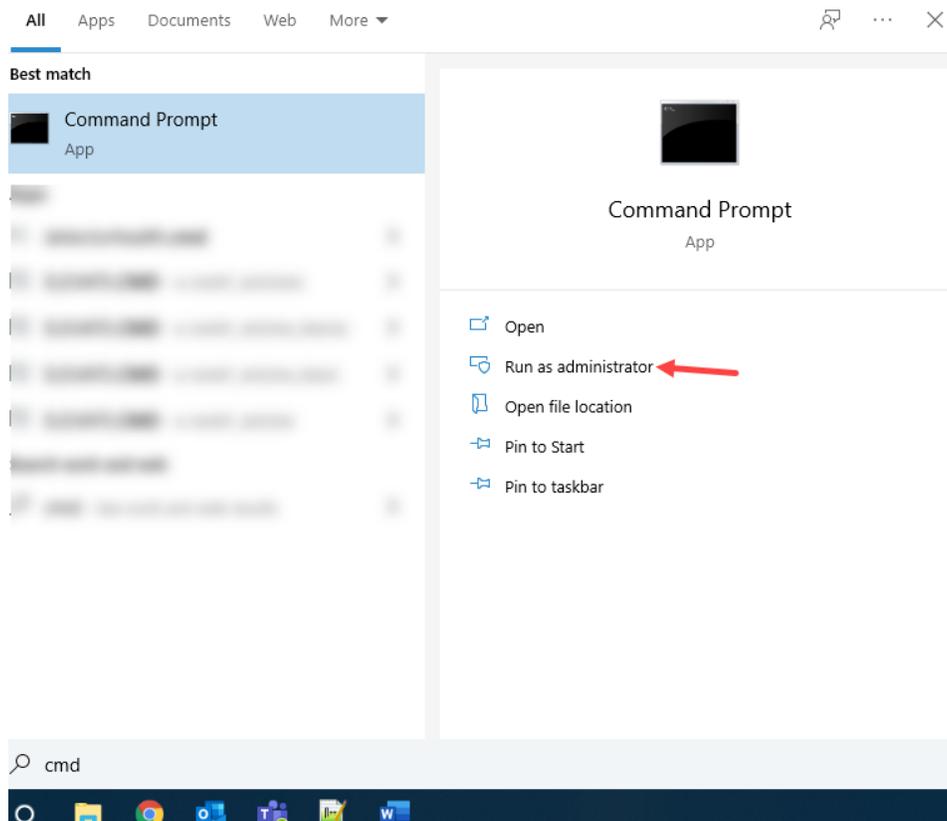
1. Exit the Hologic application and access the Windows desktop.
2. Refer to the Mitigation Procedure later in this bulletin.

### Mitigation Procedure:

***Note: Do not attempt to perform the mitigation procedure below without first ensuring that you are logged into the Windows Operating System as a user with administrative privileges.***

Use the following steps to remove the impacted services from the system.

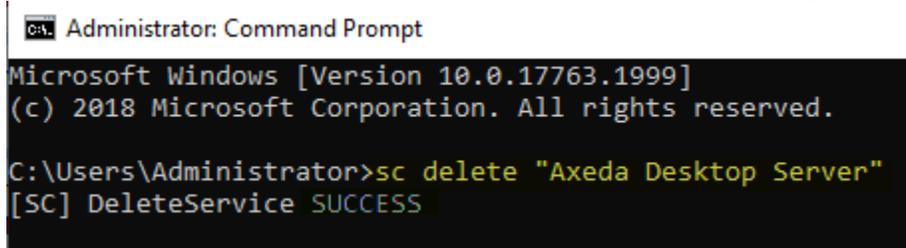
1. Search the Start menu for CMD and select Run as administrator, as shown in the figure below.



*Note: The screen shot is for Windows 10. Other Windows Operating System screens might look different.*

## Technical Bulletin (cont.)

- At the prompt, type: `sc delete "Axeda Desktop Server"` (make sure to include the quotation marks as shown) and hit the Enter key, as shown in the figure below.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1999]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sc delete "Axeda Desktop Server"
[SC] DeleteService SUCCESS
```

- At the prompt, type: `sc delete HologicConnectService.exe`, and hit the Enter key.
- At the prompt, type: `sc delete tvnserver`, and hit the Enter key.
- Close the Command prompt.
- Open File Explorer and delete the following files from the specified directories.
  - C:\Program Files (x86)\Hologic\Connect\Axeda Desktop\AxedaDesktopServer.exe
  - C:\Program Files (x86)\Hologic\Connect\connector\ERemoteServer.exe
  - C:\Program Files (x86)\Hologic\Connect\connector\xBase39.dll
- Reboot the computer.
- Refer to the “Exiting the Hologic application” earlier in this bulletin.
- Open Services.msc from the Control Panel or by searching Services in the Start menu.
- Confirm the following services are not present:
  - TightVNC Server
  - Hologic Connect
  - Axeda Desktop Server

### **Support:**

If there are any questions or concerns regarding this communication, please contact your local Hologic support representative or Hologic Technical Support. Alternatively, country-specific telephone and email contact information for Technical Support can be found at [www.hologic.com/support](http://www.hologic.com/support).