Title:	**Carestream Product Security Advisory – Access:7 – PTC Axeda**
Advisory ID:	CARESTREAM-2022-01
Issue Date:	03/08/2022
Last Revision Date:	03/14/2022
Revision #:	3

Vulnerability Summary:
The security research firm CyberMDX has discovered 7 vulnerabilities in Axeda remote management software from PTC. These vulnerabilities impact versions of Axeda prior to 6.9.2.

Carestream leverages the Axeda client for its Smart Link Remote Management Services (RMS). Most Carestream products incorporate Smart Link and most of those installations are using vulnerable versions of Axeda, although the vulnerabilities are mitigated on most devices. See below for more details.

Vulnerability Status Summary:
Only devices actively connected to Carestream Smart Link Remote Management Services (RMS) are impacted by these vulnerabilities. Carestream has created and validated security updates for these devices. As of March 10, 2022, 99+% of impacted devices have been remotely updated through RMS. Devices should be powered on and network connected to facilitate automatic patching. Remaining devices are patched as they become available online. Carestream service will proactively address any vulnerable systems that fail to automatically update with on-site visits if necessary. No customer intervention is required.

Currently, there is no indication that these vulnerabilities are being used maliciously to attack any vendor devices.

CVE(s):

ID	CVSS 3.0	Axeda Component	Vulnerability
CVE-2022-25246	9.8	AxedaDesktopServer.exe	Successful exploitation of this vulnerability could allow a remote authenticated attacker to take full remote control of host operating system via Remote Desktop Connection.
CVE-2022-25247	9.8	ERemoteServer.exe	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to obtain full file-system access and remote code execution.
CVE-2022-25248	5.3	ERemoteServer.exe	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to access live event text log information.
CVE-2022-25249	7.5	xGate.exe	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to obtain file system read access via web server.
CVE-2022-25250	7.5	xGate.exe	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to shut down the xGate.exe service.
CVE-2022-25251	9.8	xGate.exe	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to read and modify the Axeda agent's configuration.
CVE-2022-25252	7.5	xBase39.dll	Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to crash the Axeda agent.

Links for more information:

- https://www.ptc.com/en/support/article/CS363561
- https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01
- https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- https://www.cybermdx.com/research/vulnerability-access7-220308/
- https://www.forescout.com/resources/access-7-supply-chain-vulnerabilities-can-allow-unwelcomed-access-to-your-medical-and-IoT-Devices

Vulnerability Details:
Vulnerabilities were discovered in 3 Axeda client services:

- **AxedaDesktopServer** – This component is not present on Carestream devices. PTC recommendations for unique passwords per device do not apply when this service is not included.
- **ERemoteServer** – This component may be present but is not running on Carestream devices. The security update will remove this file if it is present.
- **xGate** – This component may be present and may be running on Carestream devices.

In order for Axeda vulnerabilities in Carestream devices to be exploitable:

- The device must have a vulnerable Axeda client installed.
    - Carestream systems with DirectView, ImageView, DryView, Image Suite, and MyVue Center Kiosk systems shipped or updated since 2012 contain the Axeda client. Prior to 2012, Carestream used a different remote service tool.
    - Axeda client versions 6.9.2 and later do not have these vulnerabilities.
      Note that Axeda client versions 6.9.2 and later do not support older operating systems and other mitigations (loopback configuration - below) must be applied instead.
- The device must be configured to utilize Carestream Smart Link remote service.
    - The xGate service does not start unless Smart Link has been configured for remote service. AxedaDesktopServer and ERemoteServer services are never running.
    - Note: By default, Smart Link is not configured and no services are running. Only when RMS is configured will the xGate service be running.
- The device must be configured to allow external connections to Axeda services on the medical device from other devices on the hospital network.
    - This is not the configuration for any current Carestream product. All services are configured for loopback internal communication only. All systems use a secure tunnel to communicate with the Axeda servers and internal services such as xGate are routed internally through this tunnel. No inbound communication is possible, mitigating remote exploitation of the vulnerabilities.
    - PTC's security advisory states that using Axeda client version 6.9.1 or later and configuring the system for loopback internal communication only will mitigate the vulnerabilities. All Carestream systems using Axeda client 6.9.1 or later are configured for loopback internal communication only.
    - Some older versions of the Axeda client may be configured to allow incoming connections and may be vulnerable.
- The device's software firewall or a network firewall must not be configured to block incoming connections to Axeda services on the medical device.

Patch Availability:

For Carestream DirectView V5.7G or later, ImageView, Image Suite 4.0.8.0 and later, and My Vue Kiosk systems:
All existing systems are configured for internal communication (loopback) only and the vulnerabilities are not remotely exploitable. Patches are provided for full vulnerability remediation purposes only.

Carestream has updated the Smart Link Remote Management Service to utilize the latest release of the Axeda client (6.9.3) which remediates these vulnerabilities. This version is also configured for loopback internal communication only which does not permit incoming connections to Axeda services. This version of Smart Link has been validated and released for all Carestream products and is available for installation.

99+% of all Smart Link Remote Management Service (RMS) connected systems have been patched. RMS connected systems should remain powered on and network connected overnight to facilitate automated patching. Additionally, Carestream is patching all systems that contain Smart Link that are not connected to Remote Management Service (RMS) based on accessibility.

For Carestream DirectView systems V5.7F, Image Suite 4.0.7.0 and earlier, or earlier and DryView Printers running Windows XP Embedded or Windows Embedded 2009:
Axeda clients version 6.9.2 and later do not support the Windows XP Embedded or Windows Embedded 2009 operating systems and some older Windows 7 systems. Note: Windows Embedded 2009 is a repackage of Windows XP Embedded SP3. The most recent version of the Axeda client which may be used for these systems is 6.9.1.

PTC's guidance for these systems to upgrade the Axeda client to 6.9.1 and to ensure the systems are configured for internal communication (loopback) only, mitigating remote exploitation of the vulnerabilities.

For these systems, Carestream has updated the Smart Link Remote Management Service to utilize Axeda client 6.9.1 and configured the services for internal communication (loopback) only, which mitigates remote exploitation of the vulnerabilities. This version of Smart Link has been validated and released for all Carestream products and is available for installation.

99+% of all Smart Link Remote Management Service (RMS) connected systems have been patched. RMS connected systems should remain powered on and network connected overnight to facilitate automated patching. Carestream service will proactively address any vulnerable systems that fail to automatically update with on-site visits if necessary. No customer intervention is required. Additionally, Carestream is patching all systems that contain Smart Link that are not connected to Remote Management Service (RMS) based on accessibility.

For Carestream DryView Printers running Linux:
All systems are currently configured for internal communication (loopback) using Axeda client version 6.9.1 and are not remotely exploitable per the Axeda security advisory. No action is required for these systems.

Complete list of Carestream Products and Impact Status:

X-Ray Systems utilizing ImageView Software Platform

- All versions are mitigated. These systems are configured for loopback internal communication only and do not accept external connections.
    - DRX-Evolution
    - DRX-Evolution Plus
    - DRX-Ascend
    - Q-Rad Systems
    - DRX Compass
    - DRX-1 System
    - DRX-Revolution
    - DRX-Revolution Nano
    - DRX-Mobile Retrofit
    - DRX Mobile Upgrade Solutions
    - DRX Mobile Upgrade Solutions
    - DRX-Transportable
    - DRX-Transportable Lite
    - OnSight 3D Extremity System
    - Q-Vision *

X-Ray Systems utilizing DirectView Software Platform

- Versions 5.1 – 5.3 systems do not include Axeda components and are therefore not vulnerable.
- Versions 5.4 – 5.7F accept external connections and are vulnerable if Smart Link Remote Management Services (RMS) has been configured.
- Versions 5.7G – 5.7K are mitigated. These systems are configured for loopback internal communication only and do not accept external connections.
    - CR825
    - CR850
    - CR950
    - CR975
    - DIRECTVIEW Max CR System
    - DIRECTVIEW Classic CR System
    - DIRECTVIEW Elite CR System
    - DIRECTVIEW Remote Operations Panel
    - DR 3000
    - DR 3500
    - DR 7500
    - DR 9500
    - DRX-Evolution
    - DRX-Ascend

- DRX-Innovation
- Q-Rad Systems
- DRX-1 System
- DRX-Revolution
- DRX-Mobile Retrofit
- DRX-Neo
- DRX Mobile Upgrade Solutions
- DRX-Transportable
- DRX-Transportable Lite
- Motion Mobile *
- ODYSSEY *
- QUEST *
- Tech Vision *

Image Suite Systems

- Versions 4.0.7.0 and earlier accept external connections and are vulnerable if Smart Link Remote Management Services (RMS) has been configured.
- Versions 4.0.8.0 and later are mitigated. These systems are configured for loopback internal communication only and do not accept external connections.
    - CRescendo Classic Image Suite
    - CRescendo WAIV Series with Touch Screen
    - CRescendo Vita Image Suite
    - CRescendo Max
    - Vita CR System
    - Vita Flex CR System
    - DRive
    - PRO Detector Systems

Print Kiosk Systems

- All versions are mitigated. These systems are configured for loopback internal communication only and do not accept external connections.
    - MyVue Center K3 Kiosk

Print Systems utilizing DryView Software Platform

- Linux based systems are mitigated. Linux systems are configured for loopback internal communication only and do not accept external connections.
- Windows XP Embedded and Windows Embedded 2009 based system accept external connections and are vulnerable if Smart Link Remote Management Services (RMS) has been configured.
    - DRYVIEW 5700
    - DRYVIEW 5800
    - DRYVIEW 5850

- DRYVIEW 5950
- DRYVIEW 6800
- DRYVIEW 6850
- DRYVIEW 6950

Products that do not contain Smart Link and are not impacted

- DRX-Excel
- OMNI Products
- X-Ray Detectors
- INDUSTREX NDT Systems
- QV-800 Digital Universal System *
- RAD-X Systems *

* - Indicates analog systems that are typically not connected to a network

Mitigating the risk for the vulnerability:
Using a network firewall to block the ports associated with the Axeda xGate.exe client service will mitigate the vulnerabilities:

xGate Function	Port
Kill Signal	TCP 3011 incoming to the medical device
Configuration Get / Set	TCP 3031 incoming to the medical device
HTTP Configuration	TCP 9420 incoming to the medical device

Note that these port numbers differ from the CyberMDX advisory. Carestream devices do not run the AxedaDesktopServer (VNC) or ERemoteServer services. Also, some default ports are configurable and have been altered by Carestream.

Note that blocking these ports will not prevent the use of Smart Link Remote Management Services (RMS).

For Further Information:
Contact the Carestream Center of Excellence (COE) if you have any additional questions. Service and support contacts can be found on Carestream's website at:
https://www.carestream.com/en/us/services-and-support

Please contact your Carestream sales representative to inquire about updating to the latest version of software.

Carestream Product Security Guidance:
Carestream continuously evaluates the cybersecurity strategy of its products and often includes security patches and improvements with each software release. In order to maximize the resilience of your equipment, Carestream recommends customers keep their devices current by upgrading to the latest software release available for the product(s).
Carestream strongly recommends customers apply a layered security approach to protect all of their medical devices including Carestream equipment. Recommendations include but are not limited to:

- **Updates:** Apply software and security updates to the medical device when available.
- **Encryption:** Leverage Data at Rest and Data in Transit solutions to protect confidential data and the security of the system.
- **Physical Security:** Physically limit access to equipment when possible.
- **Role Based User Access**: Limit access to the equipment to authorized users only and minimize user privileges by role.
- **Network Isolation and Segmentation:** Firewalls, network segmentation, and/or virtual LANs should be used and configured to limit network communication of medical devices to only the addresses and ports required to support your workflow.
- **Endpoint & Network Monitoring:** Monitor the actions of devices at the endpoint and on the network through firewall, intrusion detection, endpoint audit logs by forwarding these logs to a Security Information and Event Management (SIEM) system.
- **Intended Use:** Only use Carestream products for intended use – do not check personal email, browse the internet, or install applications not required for the medical device

Updates to this advisory:
Future updates to this advisory will be posted to Carestream's website:
https://www.carestream.com/services-and-support/cybersecurity-and-privacy