**Title:** Critical vulnerabilities in devices using code from Treck Software
**Advisory ID**: CARESTREAM-2020-03
**Issue Date**: June 16, 2020
**Last Revision Date**: August 26, 2020
**CVE(s)**: CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11901, CVE-2020-11902, CVE-2020-11904, CVE-2020-11899, CVE-2020-11903, CVE-2020-1905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11909, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914, CVE-2020-11908

## Vulnerability Information

### *What is the Ripple20 vulnerability?*

Ripple20 is a set of 19 vulnerabilities found on the Treck TCP/IP stack. Four of the Ripple20 vulnerabilities are rated critical, with CVSS scores over 9 and enable Remote Code Execution. One of the critical vulnerabilities is in the DNS protocol and may potentially be exploitable by a sophisticated attacker over the internet, from outside the network boundaries, even on devices that are not connected to the internet.
For additional information on the vulnerabilities please visit: https://www.jsof-tech.com/ripple20/

### *Are Carestream products vulnerable:*

After reviewing information provided by Carestream suppliers and using several different tools designed to detect Ripple 20 vulnerabilies, Carestream has determined that none of its products are impacted by these vulnerabilities.
Carestream will continue to monitor all available information for this and other vulnerabilities and will publish or update the product security advisories as necessary.

As part of the Ripple20 investigation, Carestream identified best practices / compensating controls to reduce the attack surface of some CR systems to reduce the risk for any potential vulnerabilities discovered in the future. Please see the **Attack Surface Reduction** section below for more information.

### *Updates to this advisory:*

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

## Carestream Guidance on Protecting Equipment from Malware

Carestream continuously evaluates the cybersecurity strategy of its products and as such often includes security patches and improvements with each software release. In order to maximize the resilience of your equipment, Carestream recommends customers keep their device's 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:

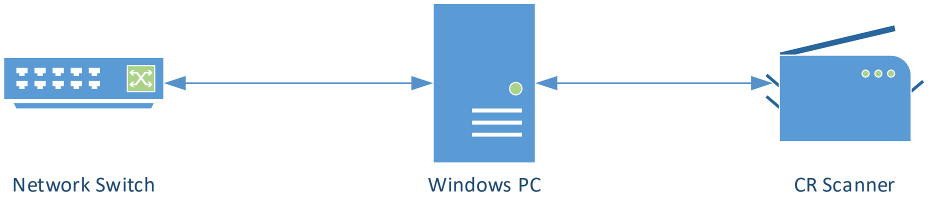
• **Physical Security**—Physically limit access to equipment when possible.

• **Role Based User Access**—Limit access to the equipment to authorized users only and minimizing 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.
- **Network Monitoring**—Monitor the actions of devices on the network through firewall, intrusion detection, and SIEM (Security Information and Event Management) logs

## Attack Surface Reduction

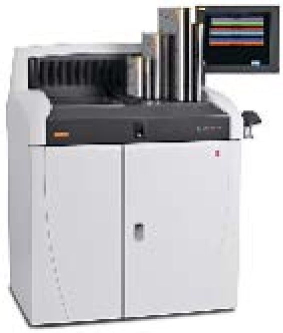
CR scanner devices are used to acquire and send CR images to a Windows PC. Typically, these CR scanners are typically directly connected to a Windows PC that has 2 network adapters – one connected to the CR scanner and one connected to the customer network. The CR scanner itself is not connected to the rest of the network which greatly reduces the attack surface of the system and the risk of any potential vulnerabilities discovered in the future.

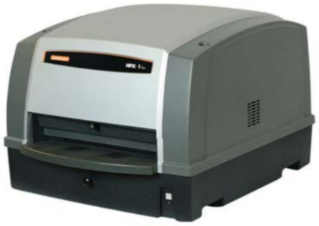


If your CR scanner devices are connected to your network, then it is highly recommended that they be modified to operate in direct connect mode. To determine if your CR scanner is connected to your network, see the instructions below.

***Identifying Medical Devices That May Benefit From This Modification:***

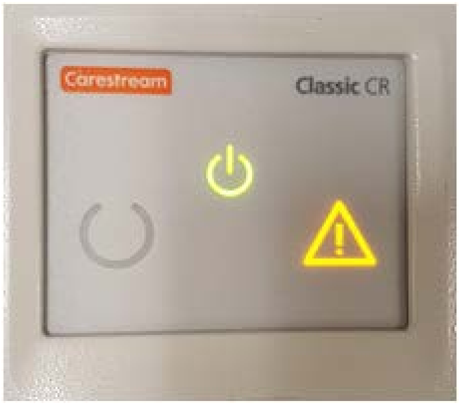
The Carestream CR 975, Max CR, HPX Pro, and HPX-One systems must be direct connected and do not require any modification.  Please see the pictures below to assist with identification:



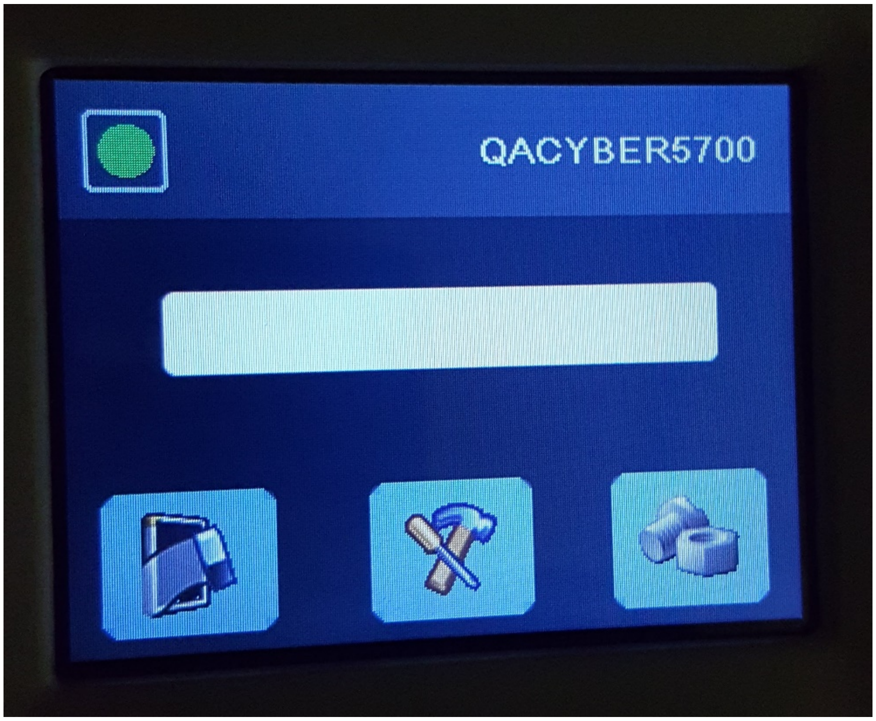


Older Carestream Classic CR and Elite CR systems may not be direct connected by default and may benefit from this modification.  Please see the picture below to assist with identification (notice the display is circled for emphasis as this will be used in the next step):

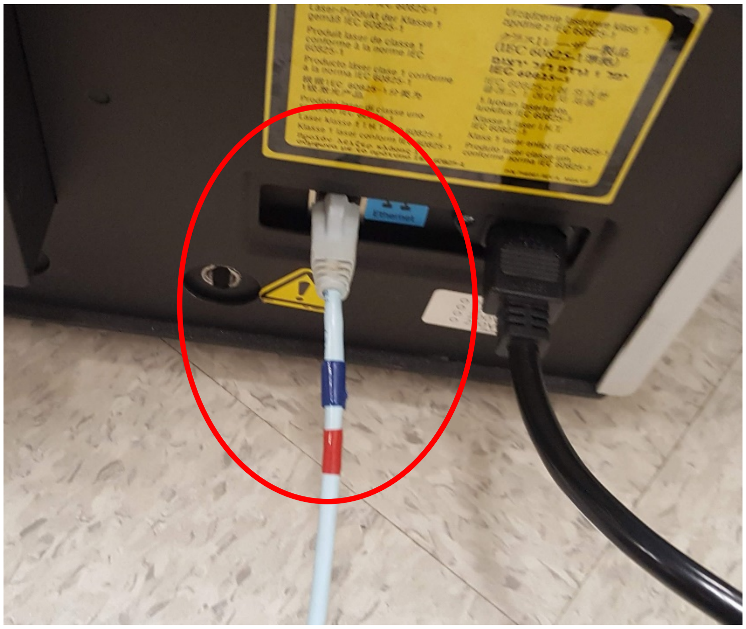
If the display on the Carestream Classic CR or Elite CR looks like the picture below then the device must already have the compensating control of the direct connect mode configuration and no further action required.



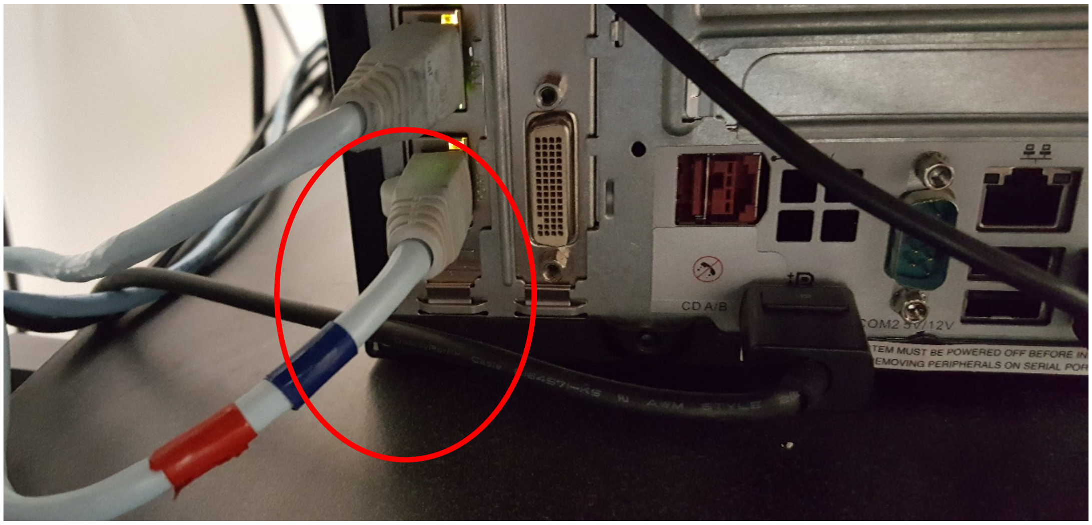
If the display on the Carestream Classic CR or Elite CR looks like the picture below then the device *may not* have the compensating control of the direct connect mode configuration.Further identification is required in the following steps:



It is possible the CR scanner is connected to your network.  Check the back of the equipment for a standard network cable as seen in the picture below:



Follow the cable to confirm it is connected to the back of a PC as shown below, not to a network port on the wall or other network device:


CD A/B
COM2 5V/12V
SYSTEM MUST BE POWERED OFF BEFORE IN
REMOVING PERIPHERALS ON SERIAL POR

If the standard network cable is present and connects the device to a PC then the compensating control of the direct connect mode configuration is in place andno further action required at this time.

If the standard network cable DOES NOT connect the device to a PC then the compensating control of the direct connect mode configuration is NOT in place.  Please contact Carestream Service to receive assistance in making the desired modification of direct connecting the CR scanner to the Windows PC.

| Carestream Health<br>Global Customer Care Service & Support |
|---|
| USA Only: 1-800-328-2910<br>Outside the USA: 585-627-1864<br>Canada: 1-866-927-1017 |
| Outside the USA and Canada: Contact your local Shared Service Center (SSC) |