Title: **Embedded TCP/IP Network Stack Vulnerabilities**
Urgent/11, Ripple20, Amnesia:33, Number:Jack, Name:Wreck
Advisory ID: CARESTREAM-2021-03
Issue Date: 04/15/2021
Last Revision Date: 04/15/2021
Revision #: 1

Vulnerability Summary:
This advisory covers five different sets of common vulnerabilities found in TCP/IP network stacks typically used by embedded systems, including medical devices. There are over 80 vulnerabilities, with many critical vulnerabilities allowing for remote code execution over the network.

Vulnerability Set	# Impacted TCP/IP Stacks / Embedded OS	# CVEs	Link for more information
Urgent/11	6	11	https://www.armis.com/urgent11/
Ripple20	1	19	https://www.jsof-tech.com/disclosures/ripple20/
Amnesia:33	6	33	https://www.forescout.com/research-labs/amnesia33/
NUMBER:JACK	9	9	https://www.forescout.com/company/blog/numberjack-forescout-research-labs-finds-nine-isn-generation-vulnerabilities-affecting-tcpip-stacks/
NAME:WRECK	4	9	https://www.forescout.com/research-labs/namewreck/

Some Carestream CR devices make use of the Green Hills Operating System which leverages a modified version of the Treck TCP/IP Network stack. In 2020, JSOF discovered that the Treck network stack contains 19 different security vulnerabilities. After consulting with Green Hills and leveraging the Tenable Nessus and JSOF vulnerability scanners, Carestream has determined that its CR devices are not vulnerable to the Ripple20 vulnerabilities. Carestream has also determined that the other 4 sets of vulnerabilities do not apply to any Carestream devices.

As part of this investigation, it was determined that some CR devices could benefit from a network modification to reduce the attack surface of the device. See below for more information to determine if your systems may benefit from this modification.

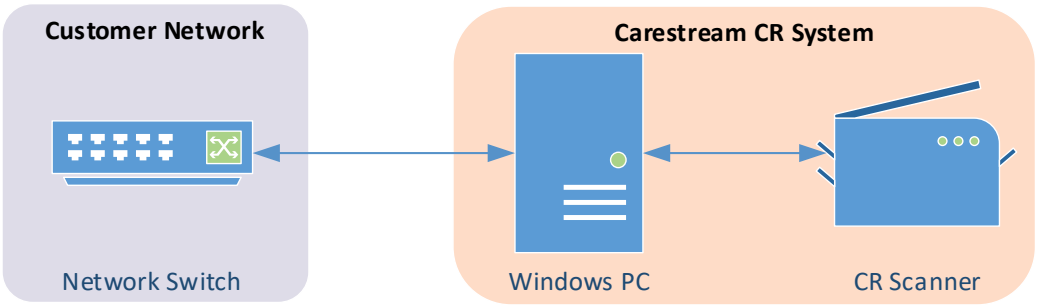
This product security advisory supersedes the following TCP/IP Network Stack advisories:

CARESTREAM-2019-02 CARESTREAM-2019-03	Critical vulnerabilities in devices using VxWorks OS - URGENT/11
CARESTREAM-2020-03	Critical vulnerabilities in devices using code from Treck Software – Ripple20

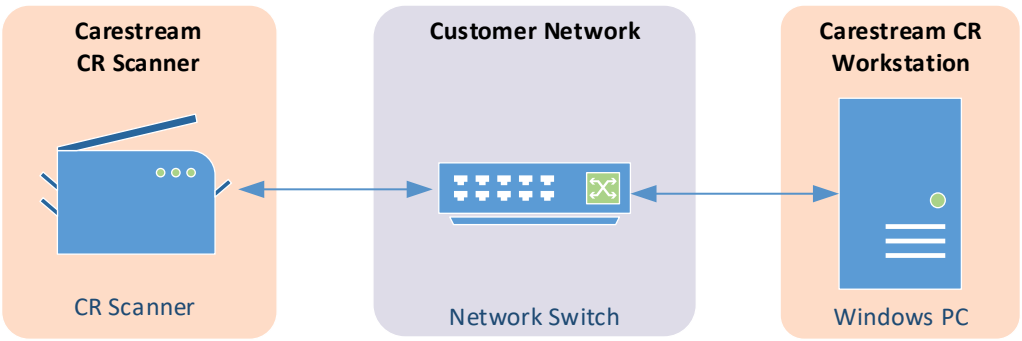
Reducing the Attack Surface of Carestream CR Systems

CR scanner devices are used to acquire and send CR images to a Windows PC. Typically, these CR scanners are directly connected to a Windows PC with 2 network adapters. The CR scanners are not connected to the rest of the network which greatly reduces the attack surface of the embedded CR scanner.

Preferred CR System Configuration – Direct Connect Mode



Alternate CR System Configuration – Through Customer Network



See the instructions below to determine if your CR scanner is connected through your network. If your CR scanner devices are connected through your network, then it is highly recommended that they be modified to operate in direct connect mode. Contact Carestream Service or your service provider for assistance in converting your CR system to direct connect mode.

Identifying CR Devices connected through the Customer Network

Carestream CR 975, Max CR, HPX Pro, and HPX-One systems may only be direct connected and cannot be routed through the customer network. No further action is required if you have these devices. Please see the picture below to assist with identification.

CR 975 / MAX CR

HPX Pro / HPX-One

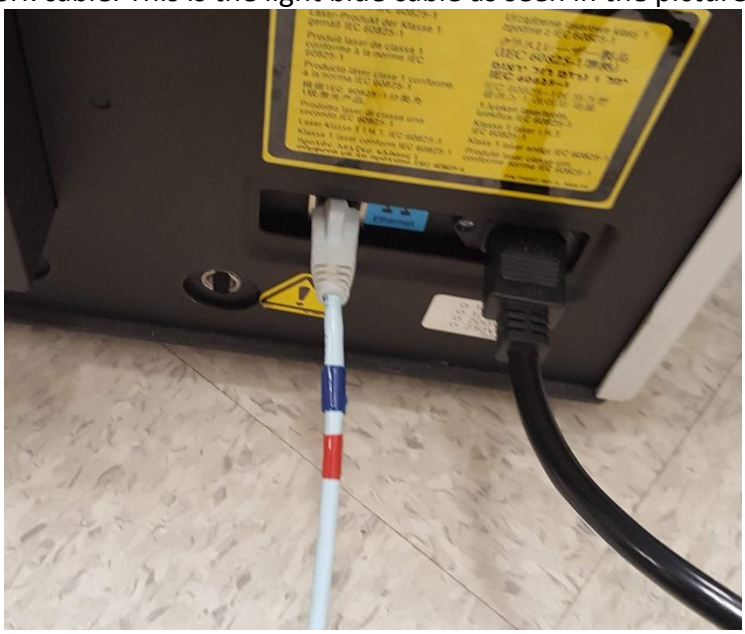
Carestream Classic CR and Elite CR systems with a built-in display might be connected through the customer network. Please see the picture below to assist with identification.
On your Carestream Classic or Elite CR system, examine the area circled in red below.

If the display on the Carestream Classic CR or Elite CR looks like the picture below on the left, then that system may only be direct connected and cannot be routed through the customer network. No further action is required. If your device has a built-in display as shown below on the right, then the device might be routed through your network.

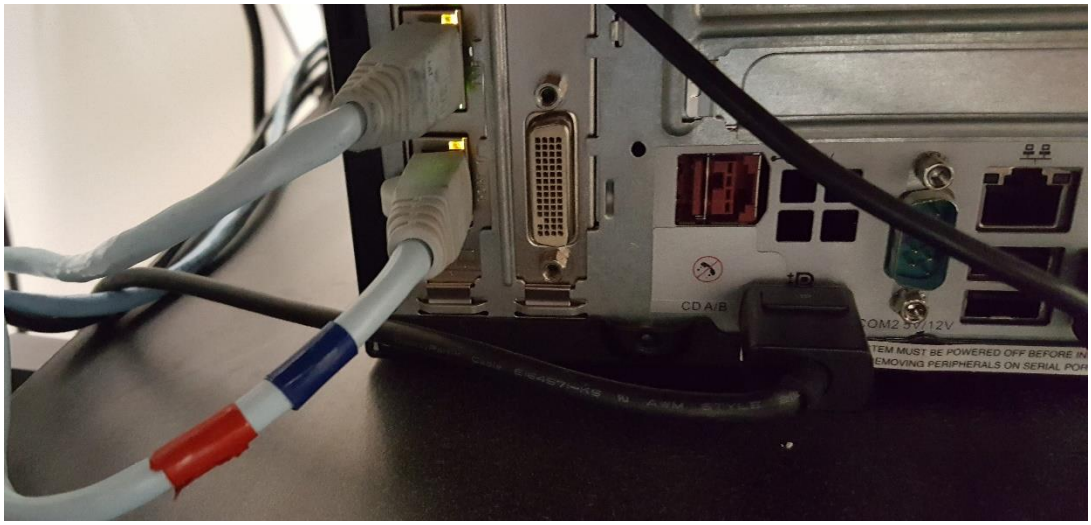
Must be Direct Connected

May not be Direct Connected

For Carestream Classic and Elite CR systems with a built-in display, examine the back of the CR scanner for a network cable. This is the light blue cable as seen in the picture below.



Follow that cable to confirm it is connected to the back of a CR Workstation PC as shown below.



If the network cable from the CR scanner is connected to a network port in the wall or another network device, then your system is not operating in direct connect mode. Contact Carestream Service or your service provider for assistance in converting your CR system to direct connect mode. Do not try to alter the network configuration yourself as software settings must be changed to allow the system to operate in direct connect mode.

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