23rd March 2021

URGENT FIELD SAFETY NOTICE
MEDICAL DEVICE CORRECTION

Datascope Cardiosave Hybrid and Rescue Intra-Aortic Balloon Pumps (IABP) Cybersecurity Vulnerabilities– Ripple20

AFFECTED PRODUCT	PART NUMBER	DISTRIBUTION DATE
Cardiosave Hybrid IABP **Cardiosave Rescue IABP**	All	All

PLEASE FORWARD THIS INFORMATION TO ALL CURRENT AND POTENTIAL CARDIOSAVE HYBRID and CARDIOSAVE RESCUE IABP USERS WITHIN YOUR HOSPITAL / FACILITY.

IF YOU ARE A DISTRIBUTOR WHO HAS SHIPPED ANY AFFECTED PRODUCTS TO CUSTOMERS, PLEASE FORWARD THIS DOCUMENT TO THEIR ATTENTION FOR APPROPRIATE ACTION.

Dear Customer,

Datascope/Getinge is initiating a voluntary Medical Device Correction for the Cardiosave Hybrid and Cardiosave Rescue Intra-Aortic Balloon Pump (IABP) due to cybersecurity vulnerabilities in a widely used low-level TCP/IP software library developed by Treck, Inc. that may result in a loss of communication to the Hospital Information System/Clinical Information System (HIS/CIS).

The inability to transmit therapy and waveform data from the Cardiosave IABP to the electronic record (HIS/CIS) does not impact the acute treatment of a patient on support.

Our records indicate that your facility has received one or more of the Cardiosave IABP units.

Identification of the issue:

On June 19th of 2020, the JSOF research lab published a series of cybersecurity vulnerabilities called Ripple20[1]. The publication consisted of nineteen (19) vulnerabilities that affects hundreds of millions of Ethernet/Internet connection capable devices.

[1] https://www.jsof-tech.com/ripple20/

Getinge's investigation revealed that five (5) of the nineteen (19) vulnerabilities may affect the operating system in Cardiosave IABP devices. If any of the vulnerabilities were exploited, Ethernet communication would be lost, and the Cardiosave will not be able communicate to the Hospital Information System/Clinical Information System (HIS/CIS) to send therapy and waveform data.

Although it will not send therapy and waveform data to the HIS/CIS, the Cardiosave IABP will still deliver therapy to the patient as intended, and there will be no degradation in performance.

The five vulnerabilities are listed in the table below:

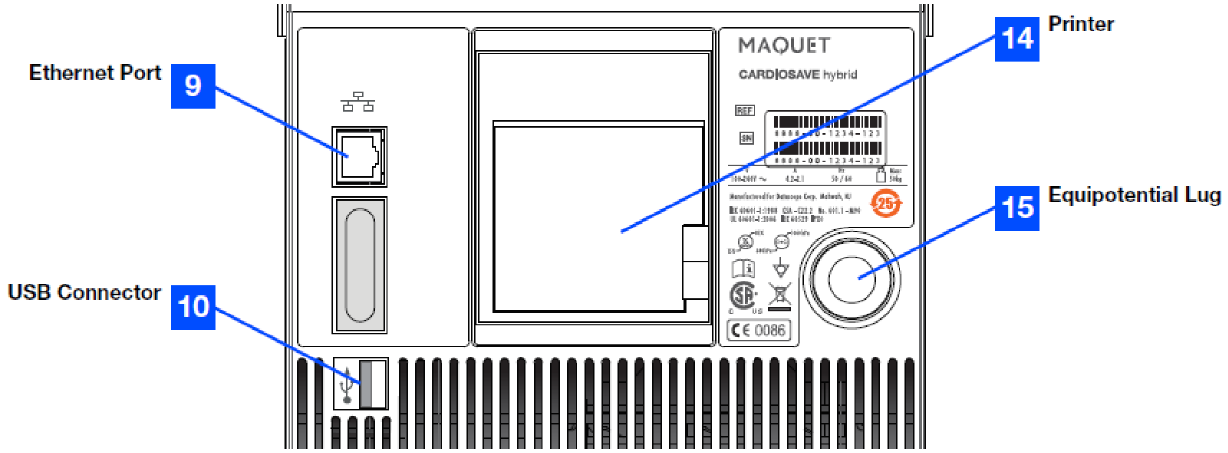
Vulnerability	Details
CVE-2020-11896	Improper handling of length parameter in IP4/UDP.
CVE-2020-11906	Improper Input Validation in Ethernet Link Layer component
CVE-2020-11907	Improper handling of length parameter inconsistency in TCP component
CVE-2020-11911	Improper access control in ICMPv4.
CVE-2020-11914	Improper input validation in ARP component

It is important to note that there have been no adverse events or deaths attributed to this issue.

Interim Immediate actions to be taken by User:

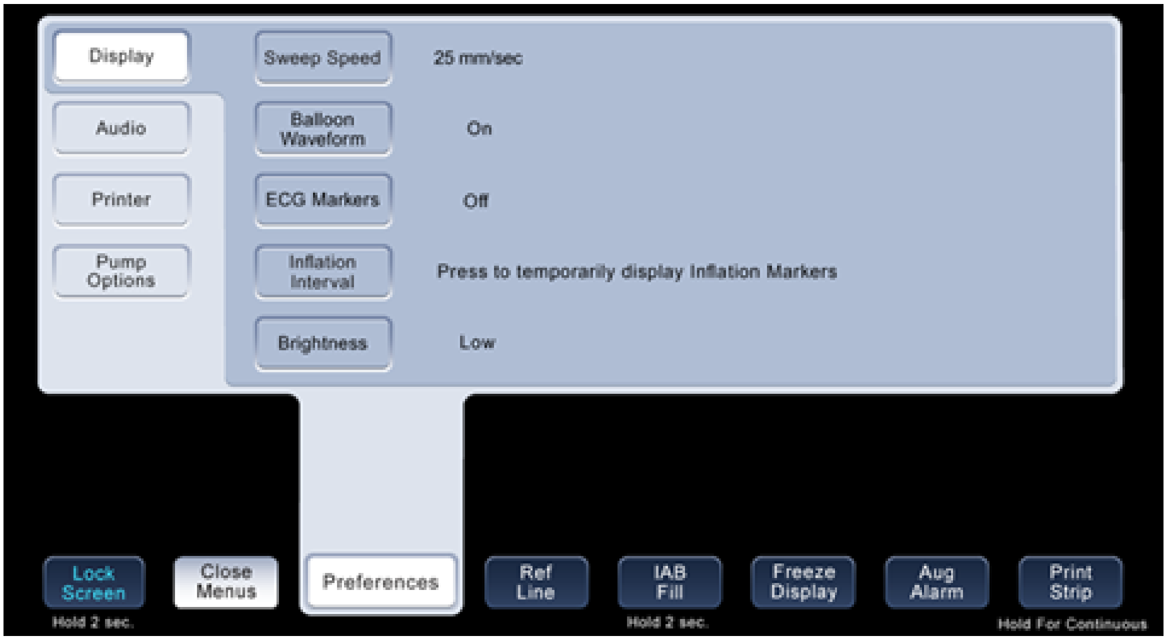
To ensure that Cardiosave Hybrid or Cardiosave Rescue are not susceptible to the Ripple20 vulnerabilities, users can disconnect the Ethernet cable from the Cardiosave Ethernet Port identified as item 9 in the image in Figure 1 below:

Figure 1 (back of Cardiosave Hybrid and Cardiosave Rescue unit)



Additionally the user can turn off Network Connections via the **Network Connections** settings in the **Pump Options** menu. Ensure that the Connection Status indicator displays red after the Network Connections are set to Off.

To access the Network Settings Menus first press the **Preferences** key on the bottom row of the Keypad display to display the **Preferences Menu**.



Sweep Speed 25 mm/sec

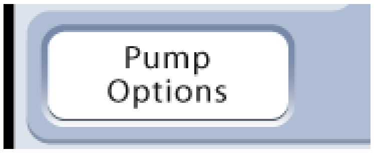
Balloon Waveform On

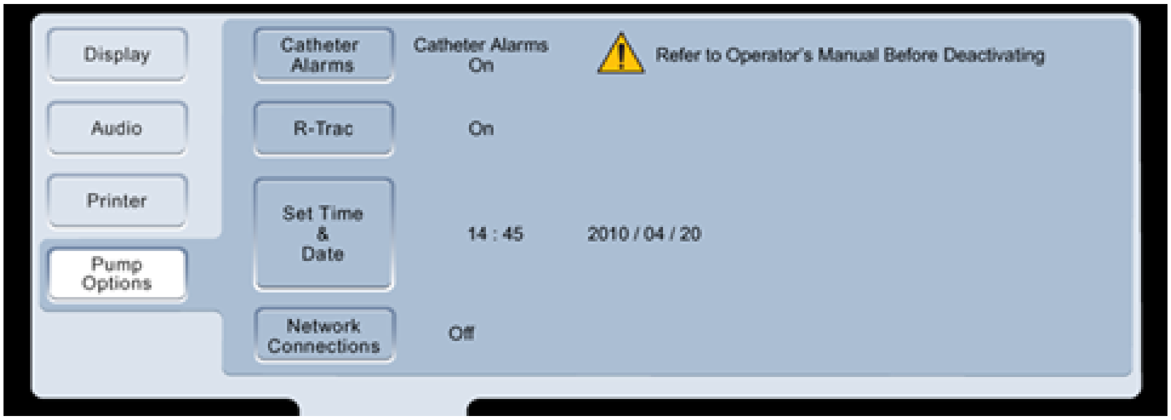
ECG Markers Off

Inflation Interval Press to temporarily display Inflation Markers

Brightness Low

Within the **Preferences Menu** select the **Pump Options** key to open the **Pump Options** sub-menu.





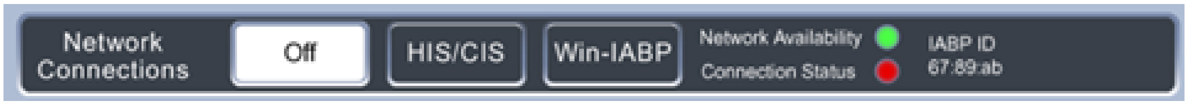
Catheter Alarms Catheter Alarms On ⚠ Refer to Operator's Manual Before Deactivating

R-Trac On

Set Time & Date 14 : 45 2010 / 04 / 20

Network Connections Off

With the **Pump Options** Menu open select the **Network Connections** key to access the network options.

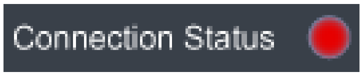


Network Availability 🟢

Connection Status 🔴

IABP ID 67:89:ab

Select the **Off** key and confirm that the **Connection Status** indicator displays red.



These actions will isolate Cardiosave from any potential external network based vulnerabilities. Cardiosave does not support any other network connection types other than the direct connected Ethernet cables.

Corrective Action:

Datascope/Getinge is currently developing a software correction to address this issue. A Datascope/Getinge service representative will contact you to schedule the installation of the updated software. This work will be done at no cost to your facility.

Please complete and sign the attached URGENT FIELD SAFETY NOTICE MEDICAL DEVICE CORRECTION– RESPONSE FORM (page 5) to acknowledge that you have received this notification. Return the completed form to Datascope/Getinge by e-mailing a scanned copy to iccomplaints.uki@getinge.com.

We apologize for any inconvenience this Medical Device Correction may cause. If you have any questions, please contact your local Datascope/Getinge representative.

This notification is being made with the knowledge of the U.S. Food and Drug Administration.

Sincerely,

H.Rajendran

Hari Rajendran
QRC Manager UKI
QRC SSU North Europe Region

23rd March 2021

URGENT FIELD SAFETY NOTICE
MEDICAL DEVICE CORRECTION
RESPONSE FORM

Datascope Cardiosave Hybrid and Rescue Intra-Aortic Balloon Pumps (IABP) Cybersecurity Vulnerabilities– Ripple20

I acknowledge that I have reviewed and understand this Urgent Medical Device Correction Letter for the affected Cardiosave Intra-Aortic Balloon Pump(s) at this facility.

I confirm that all users of the Cardiosave Intra-Aortic Balloon Pump(s) at this facility have been notified accordingly.

Please provide the required information and signature below.

Facility Representative:

Signature:________________________________ Date:____________________

Name:__________________________________ Phone:___________________

Title:___________________________ Department:________________________

Hospital Name:____

Address, City and State:____

Return the completed form by EMAIL to iccomplaints.uki@getinge.com