Subject: Single Sign-On (SSO) Password Vulnerability

Commercial name of the affected product:	Details on affected devices: Software versions impacted
Q-Stress® System	Q-Stress – 6.x.x (all versions from 6.0.0 to 6.3.1)
XScribe™ System	XScribe – 5.xx to 6.xx (all versions from 5.01 to 6.3.1)
HScribe™ System	HScribe – 5.xx and 6.x.x (all versions from 5.01 to 6.4.0)
Vision Express™ System	Vision Express – 6.x.x (all versions from 6.1.0 to 6.4.0)
Diagnostic Cardiology Suite™ (DCS)	DCS – 2.x.x (version 2.1.0)
Connex® Cardio ECG	Connex Cardio – 1.x.x (version 1.0.0 to 1.1.1)
RScribe™ System	RScribe – 5.xx, 6.xx and 7.x.x (all versions from 5.01 to 7.0.0)

FCA-identifier: FA-2021-12-001-MKE-004

Type of action:
Field Safety Notice

Date:

To: Chief Executive; Facility Risk Manager; Facility Administrator; Facility Engineer; Vigilance Manager; Biomedical Engineering; Medical Device Liaison Officer; Information Security Director

Description of the problem:
Hillrom has become aware of a software vulnerability for the above devices, which allows the entry of any username, that is provisioned in the application, without supplying a password. Entry of such username will grant access, with the same privileges of the username, to the software application within the medical device. This vulnerability occurs only when the device is activated with the Single Sign-On (SSO) feature in either stand alone, or client/server configurations.

Potential Risk
According to the security risk assessments conducted for the products, the reported vulnerability is categorized as uncontrolled, resulting in unacceptable residual risk, with an unlikely probability of critical injury due to delay of critical care or incorrect treatment.

Actions to be taken by user:
Please disable the SSO feature in the respective modality manager configuration settings. Please refer to the **Appendix A** below for instructions on how to disable SSO.

Actions to be taken by the distributor:
Please share this notification with your end users. Contact HillromMKE004OUS@Sedgwick.com to receive an editable copy of this notification. Please include your contact details on the editable copy to allow your customers contact you directly.

Contact reference person:
If you have any questions regarding this notification, please contact Hillrom Technical Support, using email or number below.

Market / Region / Country	Phone Number	Technical Support Email
Austria	43 1 79567186	emea.support@hillrom.com
Germany	+49 (0) 69 509 851 32 option 2	emea.support@hillrom.com
Switzerland	41 44 6545315	emea.support@hillrom.com
UK	+44 (0) 207 365 6780 option 2	emea.support@hillrom.com
Netherlands	+31 (0) 20 206 13 60 option 2	emea.support@hillrom.com
Spain	+34 (0) 91 749 93 57 option 2	emea.support@hillrom.com
Italy	+39 02 696 824 25 option 2	emea.support@hillrom.com
France	+33 (0)1 57 32 49 94 option 2	emea.support@hillrom.com
Sweden	+46 (0) 85 853 65 51 option 3	emea.support@hillrom.com
Ireland	+353 (0) 46 90 67 790 option 2	emea.support@hillrom.com
Eastern Europe	+353 (0) 46 90 67 790 option 2	emea.support@hillrom.com
Middle East & Africa	+353 (0) 46 90 67 790 option 2	emea.support@hillrom.com
India Subcontinent	+353 (0) 46 90 67 790 option 2	emea.support@hillrom.com
For all other countries	+353 (0) 46 90 67 790 option 2	emea.support@hillrom.com
South Africa	27 800 998 290	emea.support@hillrom.com

Transmission of this Field Safety Notice:
Please ensure this notice is circulated to all appropriate personnel. This may include, but is not limited to:

• A&E departments	• In-house maintenance staff
• Adult intensive care units	• IV nurse specialists
• All wards & Clinics	• Medical directors
• Biomedical engineering staff	• Nursing executive directors
• Clinical governance leads	• Oncology units
• Day case theatres	• Pediatric intensive care units
• EBME departments	• Risk managers
• Equipment stores & Libraries	• Supplies managers
• Health and safety managers	• Theatres

Hillrom considers patient safety and customer satisfaction our top priorities. We appreciate your time and attention in reading and disseminating this important product notification.

Yours sincerely,

Appendix A – **Instructions for Disabling Single Sign-On(SSO)**
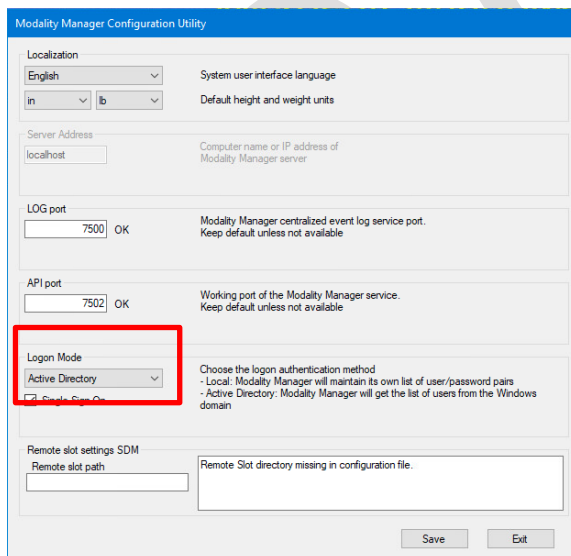
Products affected

- Q-Stress 6.x.x (all versions from 6.0.0 to 6.3.0) and XScribe 5.xx to 6.x.x (all versions from 5.01 to 6.3.0)
- HScribe 5.xx and 6.x.x (all versions from 5.01 to 6.4.0) and Vision Express 6.x.x (all versions from 6.1.0 to 6.4.0)
- RScribe 5.xx, 6.x.x, and 7.x.x (all versions from 5.01 to 7.0.0)

Notes

- This instruction is applicable for systems currently configured with the logon authentication method set to *Active Directory* and with *Single Sign On* (SSO) turned on.
- This process will briefly interrupt service. Perform these steps at an appropriate time.
- After turning off SSO, users will then need to enter their account name and password when logging into the system.

Steps to turn off SSO

1. Log into Windows as an administrator.
2. In the Start menu go to *Mortara Modality Manager* and then select *Modality Manager Configuration Tool*.
3. When prompted that services will be stopped, click *OK*.
4. The *Modality Manager Configuration Utility* window will be displayed.

5. Make sure *Single Sign On* is off.
6. Click *Save* then *Exit*.

Appendix A – **Instructions for Disabling Single Sign-On(SSO)**

Products affected
- DCS 2.x.x (version 2.1.0) and Connex Cardio 1.x.x (version 1.0.0 to 1.1.1)

Notes
- This instruction is applicable for systems currently configured with the logon authentication method set to *Active Directory* and with *Single Sign On* (SSO) turned on.
- This process will briefly interrupt service. Perform these steps at an appropriate time.
- After turning off SSO, users will then need to enter their account name and password when logging into the system.

Steps to turn off SSO
7. Log into Windows as an administrator.
8. In the Start menu go to *Hillrom* and then select *Connex Cardio Configuration Tool*.
9. When prompted that services will be stopped, click *OK*.
10. The *Modality Manager Configuration Utility* window will be displayed.
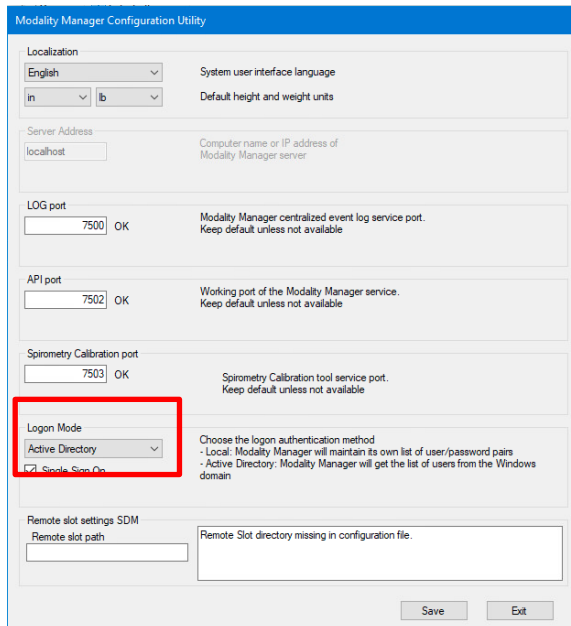
11. Make sure *Single Sign On* is off.
12. Click *Save* then *Exit*.

Response Form

Subject: Single Sign-On (SSO) Password Vulnerability
(FA-2021-12-001-MKE-004)
It is important that you return this form/receipt as acknowledgement of your receipt and provide us with the necessary information.

Please complete the following with the correct information and **return this Response Form** within 2 weeks.

Hillrom account number (if known): _____

Name of the facility: _____

Address of the facility: _____

City: Zip: Country: _____

Facility Contact Person Name: (print)

_____

Signature:_____ Date: _____/_____/_____

Title:_____Phone: _____

Email: _____

Check actions taken: (Please do not leave any questions without an answer)

We have reviewed and understand the attached <u>Field Safety Notice.</u>
□ Yes □ No

Results from the inspection of our product inventory show:
□ We do not have any potentially affected products.
□ We have affected products. Quantity _____

We confirm we have disabled the SSO feature in the impacted units in our possession.
□ Yes □ No

For Distributors only: We confirm we have shared this notification with our end users:
□ Yes □ No

Comments

_____

Response form shall be returned to <u>HillromMKE004OUS@Sedgwick.com</u> within 2 weeks.