Customer Service Bulletin

Product:	Connex® Spot Monitor (CSM), Connex® Vital Signs Monitor (CVSM), Connex® Integrated Wall System (CIWS), Welch Allyn® Service Tool (WAST), Connex® CS, Network Connectivity Engine (NCE), Service Monitor, Spot Vital Signs® 4400 Device / Spot 4400 Extended Care, Software Developer Kit (SDK)	**Date:**	2021-05-24
Subject:	Welch Allyn Product Security Vulnerability		
HW Version(s) Affected:	All	**SW Version(s) Affected:**	All **prior** to the following versions: CSM 1.52 CVSM and CIWS 2.43.02 WAST 1.10 Spot 4400 and Spot 4400 Extended Care 1.11.00 Connex CS 1.8.6 NCE 5.3 Service Monitor 1.7.0 SDK 3.2
Serial Numbers Affected:	All	**Lot or Date Code Affected:**	N/A

Classification:	Informational Only		
Distribution:	☒ Customer Care	☒ Product Service	☒ Field Service
	☐ ASPs ☐ Distributors	☒ Customers	☐ Company Confidential
Training Required:	☒ Yes ☐ No		

Summary:

Hillrom is providing a fix for a security vulnerability that has been found involving several products. This vulnerability affects products in the CSM, CVSM, CIWS, WAST, Connex CS, NCE, Service Monitor, Spot 4400, and SDK families. To reduce the security risk, Hillrom recommends the following actions.

1. For Windows based products (WAST, Connex CS, NCE, Service Monitor, SDK), customers are recommended to enable Windows Data Execution Prevention (DEP)
    a. See below for additional details and how to configure DEP

Please go to our Hillrom Responsible Disclosure page on our website to obtain our ICS-CERT on this vulnerability.

In addition, for the devices listed below, Hillrom has made the following software upgrades available.

2. **CVSM, CIWS, CSM, WAST (Service Tool), Spot 4400,** – Customers are recommended to self-upgrade devices to the following software versions as part of routine software updates:
    a. CVSM SW Version 2.43.02 or above
    b. CIWS SW Version 2.43.02 or above
    c. CSM SW Version 1.52.00 or above
    d. WAST SW Version 1.10 or above
    e. Spot 4400 and Spot 4400 Extended Care Version 1.11.00 or above (available Fall 2021)

3. **Connex CS, NCE, Service Monitor, SDK** – Customers are recommended to contact Hillrom to upgrade devices to the following software versions as part of routine software updates:
    a. Connex CS SW Version 1.8.6 or above (available Fall 2021)
    b. NCE SW Version 5.3 or above (available Summer 2021)
    c. Service Monitor SW Version 1.7.0 or above
    d. SDK SW Version 3.2 or above

Additional Details:

Data Execution Prevention (DEP) is a system-level memory protection feature that is built into the operating systems like Windows and Linux. DEP enables the system to mark one or more pages of memory as non-executable. Marking memory regions as non-executable means that code cannot be run from that region of memory, which makes it harder for the exploitation of buffer overruns.

DEP is configured at system boot according to the no-execute page protection policy setting in the boot configuration data on Windows and Linux.

DEP Configuration:

4. Open the Command window as Administrator. Do this by typing cmd in the program search field near the Start menu and selecting “run as administrator”.

5. Enter the command bcdedit.exe /set {current} nx AlwaysOn.
    a. bcdedit.exe is a Windows utility for editing boot configuration data, hence bdcedit.
    b. “/set” tells bcedit to set an option value entry in the boot configuration.
    c. “{current}” tells becedit to work with the boot configuration being used right now.
    d. “nx” is short for no execute and is the setting name for DEP in the boot configuration
    e. AlwaysOn is self-explanatory.

6. Restart the computer.

7. DEP will be turned on and all programs monitored.

8. After turning DEP to being always on or always off, it CANNOT be changed via the Data Execution Prevention tab in system settings.

Version	Sec, Pg, Para Changed	Change Made	Date Version Created	Version Created By (initials)
A	N/A	Initial Release	2021-05-24	DCS