Question or Item	Answer
Did you verify that you are using the most recent version of this form?	☒ Yes ☐ No
Date	2024-05-14
Individual creating the TSB	Matt Bell
Customer:	All
Product(s) affected:	Welch Allyn **Connex** Spot Monitor (CSM)
Hardware Version(s) affected:	ALL
Software Version(s) affected:	ALL Prior to and including CSM 1.52.00
Distribution	Customer Care, Product Service, Field Service, Company Confidential
Subject:	Baxter Product Security Vulnerability

Issue Details: Baxter is providing a fix for a security vulnerability that has been found involving CSM.

Solution/Action:

To reduce the security risk, Baxter recommends customers upgrade CSM devices to firmware v1.52.01 and the following workarounds will help reduce risk:

- Apply proper network and physical security controls.
- Ensure a unique encryption key is configured and applied to the product (as described in the Welch Allyn Connex Spot Monitor Service Manual).

1.52.01 is available to customers in the Welch Allyn Service Tool and through Smart Care Remote Management. Please refer to the following document for further details on the solution and upgrade instructions released with 1.52.01:

- CSB 80030468

Please go to our Hillrom Responsible Disclosure page on our website (https://www.hillrom.com/en/responsible-disclosures/) to obtain our ICS-CERT on this vulnerability.

END OF BULLETIN

Version	Sec, Pg, Para Changed	Change Made	Date Version Created	Version Created By (initials)
A	N/A	Initial Release	2024-05-14	MDB