



# CVE-2021-43935

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-43935  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | ics-cert@hq.dhs.gov   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-12-15 19:15:00 UTC   |
| <b>Updated</b>         | 2022-07-25 10:39:00 UTC   |
| <b>Description</b>     | The impacted products, when configured to use SSO, are affected by an improper authentication vulnerability. This vulnera |

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product   | Version | Update | Edition | Language |
|------------------|------------------------|---|---------|--------|---------|----------|
| Application      | <a href="#">Baxter</a> | <a href="#">Welch Allyn Connex Cardio</a>                                   | All     | All    | All     | All      |
| Application      | <a href="#">Baxter</a> | <a href="#">Welch Allyn Diagnostic Cardiology Suite</a>                     | 2.1.0   | All    | All     | All      |
| Hardware         | <a href="#">Baxter</a> | <a href="#">Welch Allyn Hscribe Holter Analysis System</a>                  | -       | All    | All     | All      |
| Operating System | <a href="#">Baxter</a> | <a href="#">Welch Allyn Hscribe Holter Analysis System Firmware</a>         | All     | All    | All     | All      |
| Hardware         | <a href="#">Baxter</a> | <a href="#">Welch Allyn Q-stress Cardiac Stress Testing System</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Baxter</a> | <a href="#">Welch Allyn Q-stress Cardiac Stress Testing System Firmware</a> | All     | All    | All     | All      |
| Application      | <a href="#">Baxter</a> | <a href="#">Welch Allyn Rscribe Resting Ecg System</a>                      | All     | All    | All     | All      |
| Application      | <a href="#">Baxter</a> | <a href="#">Welch Allyn Vision Express Holter Analysis System</a>           | All     | All    | All     | All      |
| Hardware         | <a href="#">Baxter</a> | <a href="#">Welch Allyn Xscribe Cardiac Stress Testing System</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Baxter</a> | <a href="#">Welch Allyn Xscribe Cardiac Stress Testing System Firmware</a>  | All     | All    | All     | All      |

## References

| Reference                                  | Source  | Link   | Tags                |
|--|---------|--|---------------------|
| Hillrom Welch Allyn Cardio Products   CISA | MISC    | <a href="http://www.cisa.gov">www.cisa.gov</a> |                     |
| CVE Program record                         | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail                   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> | canonical, analysis |

## Vendor Comments And Credit

## Discovery Credit

**LEGACY:** Hillrom reported this vulnerability to CISA

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)