

HC3 Sector Alert: Baxter Welch Allyn Vulnerabilities

Finished Intelligence
Reports

TLP:WHITE

Alert Id: 91b2d4e3

2024-06-05 13:56:13

On June 4, 2024, the Health Sector Cybersecurity Coordination Center (HC3) released a sector alert: Baxter Welch Allyn Vulnerabilities.

The alert draws attention to two vulnerabilities affecting Baxter products. CVE-2024-5176 which can be found in Baxter Welch Allyn Configuration Tool and CVE-2024-1275 affecting Baxter Welch Allyn Connex Spot Monitor (CSM). Both vulnerabilities received a CVSS v4 score of 9 or higher (CRITICAL) and are exploitable remotely.

Successful exploitation of one of these vulnerabilities could result in an impact and/or delay to patient care. While a patch is currently available for one of these vulnerabilities, a software update will not be made available for the other until Q3 2024. Mitigations and workarounds from the vendor and CISA are outlined in this Sector Alert.

Health-ISAC is distributing this report to increase your situational awareness, and encourages members to take appropriate steps to mitigate risk of these vulnerabilities being exploited by either applying available patches and/or workarounds, and continuously monitoring their networks for suspicious activity.

For additional details, please see the attached report.

Report Source(s): HC3

Release Date: Jun 05, 2024 (UTC)

Tags: CVE-2024-1275, CVE-2024-5176, Baxter Welch Allyn Connex Spot Monitor (CSM), Baxter Welch Allyn Configuration Tool, HC3

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base:

Check out our Knowledge Base for HITS integration documentation. <https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/>

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org