# Product Security Bulletin

Title: Phoenix Advisory ICSMA-20-170-03
Publication Date: June 18, 2020

Updated: June 18, 2020

In support of our mission of saving and sustaining lives, Baxter takes product security seriously. Baxter has reviewed the Phoenix product line for cybersecurity related vulnerabilities and is voluntarily disclosing the following vulnerabilities per our responsible disclosure process.

## Vulnerability Summary

The following vulnerabilities were identified in the Phoenix system. There have been no reports of the following vulnerabilities being exploited.

**CVE-2020-12048** - The Phoenix Hemodialysis device does not support data-in-transit encryption (e.g. TLS/SSL) when transmitting treatment and prescription data on the network between the Phoenix system and the Exalis dialysis data management tool. An attacker with access to the network could observe sensitive treatment and prescription data sent between the Phoenix system and the Exalis tool.

## Affected Products and Versions

The following product configurations are affected:

- Phoenix Hemodialysis Delivery System SW 3.36 and 3.40

## Mitigations

Baxter Recommends users apply the following implementation guidance:

- Ensure that medical device implementations and configurations employ cybersecurity defense in depth strategies such as:
    - Proper network segmentation- As outlined in the operating manual, ensure Phoenix machines and Exalis Server PCs reside on a dedicated subnetwork (the machines and the Exalis servers must be the ONLY devices present within it).
    - In case of remote connection (WAN) the subnetwork must be kept as dedicated by using a VPN network connection.
    - Firewalling each network segment, limiting inbound and outbound connections
    - Scanning for unauthorized network access

- Scanning for vulnerabilities and viruses

Users should also identify, analyze, evaluate and control all risks associated with integration of medical devices in an enterprise network. Subsequent changes to the enterprise network could introduce new risks and require new analysis.

## Related Information

If you observe any symptoms that are representative of these vulnerabilities, contact your service representative immediately.

*Additional resources:*

https://www.us-cert.gov/ics/advisories/icsma-20-170-03

*For more information:*

For Baxter technical support contact: 1-800-525-2623 (Prompt 2)

For questions regarding cybersecurity of Phoenix or any Baxter product contact: productsecurity@baxter.com