Product Security Bulletin

Title: PrisMax Advisory ICSMA-20-170-02
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 PrisMax 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 PrisMax. There have been no reports of the following vulnerabilities being exploited.

CVE-2020-12036 - PrisMax doesn't support data-in-transit encryption (e.g. TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system.

A threat actor with access to the network supporting PrisMax could observe sensitive data sent from the device.

CVE-2020-12035 – PrisMax doesn't support authentication when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system.

A threat actor with access to the network supporting PrisMax could execute a man-in-the-middle (MiTM) attack, allowing them to modify treatment status information.

Affected Products and Versions

The following product configurations are affected:

- PrisMax (all versions before V3.x) connected to a secondary data management system (EMR, PDMS)

Mitigations

As cybersecurity is a shared responsibility, the following guidance should be considered by the Responsible Organization during implementation:

- Physical access to the device should be limited to only authorized users.

- Prepare and perform training for personnel granted elevated privileges on the device, cautioning them against credential sharing and educating them on possible consequences of that for the patient.

- Ensure that IT maintain cybersecurity of hospital environment around device by performing following:
  - Network segmentation
  - Firewalling each network segment, limiting inbound and outbound connections
  - Scanning for unauthorized network access
  - Scanning for vulnerabilities and viruses

- Consider upgrading to PrisMaxV3 with DCM (Digital Communication Module), which supports mutually authenticated TLS tunnel to a PDMS or EMR system that is capable of implementing the latest TLS 1.2.

If a PDMS or EMR system is to be used with the device, the Responsible Organization is obliged to verify compatibility between the two systems. The Responsible Organization should identify, analyze, evaluate and control risks due to integration of PrisMax in an IT network. Subsequent changes to the IT network could introduce new risks and require new analysis. The use of a PDMS or EMR system not compatible with the PrisMax system can result in presentation of erroneous data. It is the responsibility of the physician to verify all data before prescribing any therapeutic or pharmacological action for the patient.

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-20-170-02

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