Product Security Bulletin

Title: Prismaflex Advisory ICSMA-20-170-02
Publication Date: June 18, 2020

Updated: July 14, 2020

In support of our mission of extending lives and expanding possibilities, Vantive takes product security seriously. Vantive has reviewed the Prismaflex 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 Prismaflex system. There have been no reports of the following vulnerabilities being exploited.

CVE-2020-12036 - The Prismaflex device 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 the Prismaflex system could observe sensitive data sent from the device.

CVE-2020-12035 – The Prismaflex device 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 the Prismaflex system could execute a man-in-the-middle (MiTM) attack, allowing them to modify treatment status information.

CVE-2020-12037 – The Prismaflex device contains a hard-coded service code which provides access to biomedical information, device settings, calibration settings, and network configuration. This service code is reserved for technician use.

A threat actor with access to the device could modify device settings and calibration.

Affected Products and Versions

The following product configurations are affected:

- Prismaflex (all versions)

Mitigations

Prismaflex versions SW 8.2x include the option to set a device specific service password.
Note: Prismaflex versions SW 8.2x are not available in all regions, including the U.S.

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

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 Prismaflex 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 Prismaflex 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 Prismaflex or any Vantive product contact:
global.corp.product.security@vantive.com