

Memo

|  |  |
| --- | --- |
| To: | Northwest Shelbyville Regional Hospital |
| From: | Reece Zunino |
| Date: | 11 March 2022 |
| Re: | IoT (Internet of Things) and IoMT (Internet of Medical Things) |

The following memo will describe the multiple devices utilized in the Hospital, identify discovered vulnerabilities, and secure those vulnerabilities.

**Device 1:** Alaris Plus medical syringe pumps

Include:

* The Alaris™ GH Plus syringe pump offers a range of features suited to drug therapy, blood, and blood products, including a large, clear display, intuitive user interface, integrated design, and a wide range of specialty infusion sets (Becton, Dickinson and Company, n.d.).
* CVE-2022-23612-Becton, Dickinson, and Company (BD) Alaris Plus medical syringe pumps (models Alaris GS, Alaris GH, Alaris CC, and Alaris TIVA) versions 2.3.6 and prior are affected by an improper authentication vulnerability where the software does not perform authentication for functionality that requires a provable user identity, where it may allow a remote attacker to gain unauthorized access to various Alaris Syringe pumps and impact the intended operation of the pump when it is connected to a terminal server via the serial port (CVE, 2018).
* BD recommends the following mitigations and compensating controls to reduce the risk associated with this vulnerability (CISA, 2018):
  + This attack utilizes a known vulnerability in terminal servers. Users who utilize terminal servers should understand that terminal server use is not supported (CISA, 2018).
  + Users should ensure they are operating these devices in a segmented network environment or as a stand-alone device (CISA, 2018).
  + Users should utilize connections via the Alaris Gateway Workstation docking station, which would inactivate the remote-control feature (CISA, 2018).
* My recommendation to the Hospital is to minimize any network exposure to all control systems associated with the Alaris Plus medical syringe pumps. The Hospital should also consider using VPNs within the network on all systems having to access the network remotely. This also means ensuring that all VPNs being used on the network should be up to date on all patches and updates.

**Device 2:** Patient Monitoring Systems

Include:

* Infinity Delta and Delta XL incorporate Dräger’s patented Pick and Go® technology, which enables this bedside monitor to double as a transport monitor within the Hospital. Infinity monitors provide seamless wired-to-wireless networking, so surveillance can be continuous. There’s no waiting for a transport monitor. No disconnection or reconnection of leads. No gaps in monitoring or data acquisition. As a result, all parameters that were monitored at the bedside can continue to be monitored on transport (Drager, 2016).
* CVE-2018-19010 - Drager Infinity Delta, Infinity Delta, all versions, Delta XL, all versions, Kappa, all version, and Infinity Explorer C700, all versions. A malformed network packet may cause the monitor to reboot. By repeatedly sending the malformed network packet, an attacker may be able to disrupt patient monitoring by causing the monitor to repeatedly reboot until it falls back to the default configuration and loses network connectivity (CVE, 2018).
* Dräger released fixes for these vulnerabilities in December 2018. Users can find Delta/Infinity Explorer VF10.1 software releases for affected components via Dräger Service Connect (CISA, 2019).

Dräger further advises:

* + Users are advised to review their network segmentation configuration. The Dräger Infinity Network is supposed to be either logically or physically separate from the hospital LAN (CISA, 2019).
  + Users are advised to review the Windows patch level of their Infinity Explorer. The Infinity Explorer software is verified by Dräger on a monthly basis to be compatible with all the latest operating system patches by Microsoft. Users can get the test report via their local sales representative (CISA, 2019).
* I would recommend that all Patient Monitoring Systems be taken off the network and updated to the latest updates that Drager has sent out. Once all updates have been installed, all machines must be inspected to ensure they were updated to the latest version. Once all devices have been verified, they have been updated then they can be brought back onto the network

References

Becton, Dickinson and Company. (n.d.). Alaris GH plus syringe pump with Guardrails. Advancing the world of health | BD. https://www.bd.com/en-za/our-products/infusion/infusion-devices/alaris-plus-platform-with-guardrails-safety-software/alaris-gh-plus-syringe-pump-with-guardrails

CISA. (2018, August 23). BD Alaris plus. https://www.cisa.gov/uscert/ics/advisories/ICSMA-18-235-01

CISA. (2019, January 22). Drager infinity delta. https://www.cisa.gov/uscert/ics/advisories/ICSMA-19-022-01

CVE. (2018, August 1). Cve - cve-2018-14786. CVE -CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14786

CVE. (2018, June 11). Cve - cve-2018-19010. CVE -CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19010

Drager. (2016). Infinity® MultiMed® 12 Pod. https://www.draeger.com/Products/Content/9051717\_multimed12\_pi\_en.pdf

ICS-CERT. (2019, October 9). Cve-2018-19010. NVD. https://nvd.nist.gov/vuln/detail/CVE-2018-19010

ICS-CERT. (2020, August 24). Cve-2018-14786. NVD. https://nvd.nist.gov/vuln/detail/CVE-2018-14786