BD UK
1030 Eskdale Road
Winnersh Triangle
Wokingham
RG41 5TS

bd.com/en-uk

July 2019

ATTN: Purchasing, Nursing, Pharmacy and Biomedical Staff

RE: Product Security Notification for Alaris™ Gateway Workstation and Alaris™ Gateway Workstation Web Browser User Interface

Dear Valued Customer,

BD has established a routine practice of seeking, communicating, and addressing cyber security issues in products in a timely fashion. Vulnerability disclosure is an essential component to BD's approach to transparency by enabling customers to properly manage risk through awareness and guidance.

This notification provides product security information and recommendations related to a product security vulnerability found within specified versions of the Alaris™ Gateway Workstation (Workstation) and a product security vulnerability found within the Workstation Web Browser User Interface, a web-based application. You are receiving this letter since you have been identified as a customer who utilizes an affected version of the Workstation and/or the Workstation Web Browser User Interface.

Products in Scope

Alaris™ Gateway Workstation

The Alaris™ Gateway Workstation is intended to be used to provide mounting, power and communications support to the Alaris™ Infusion Pumps range within the operating environment specified in the Directions For Use (DFU).

This notification applies to the Alaris™ Gateway Workstation, 80203UNS02-xx, 80203UNS03-xx and 80300UNS02-xx configurations with the following versions:

- 1.1.3 Build 10
- 1.1.3 MR Build 11
- 1.2 Build 15
- 1.3.0 Build 14
- 1.3.1 Build 13

There have been no reported exploits of this vulnerability. This does not impact the latest firmware version 1.3.2 nor version 1.6.1.

Additionally, this notification may apply to the following products, with software version 2.3.6 and below, only if the products are utilized with the specific versions of the Workstation:

- Alaris™ GS (not actively supported)
- Alaris™ GH
- Alaris™ CC
- Alaris™ TIVA

Only software versions for 2.3.6 and below are impacted. Software version 2.3.6 was released in 2006. These pumps were previously sold under the Asena brand. This does not apply to Alaris™ System devices.

Alaris™ Gateway Workstation Web Browser User Interface
This notification applies to the Alaris Gateway Workstation Web Browser User Interface, a web-based application used to configure the Alaris Gateway Workstation for the following versions only:

- 1.0.13
- 1.1.3 Build 10
- 1.1.3 MR Build 11
- 1.1.5
- 1.1.6

There have been no reported exploits of this vulnerability.
This does not impact the latest firmware version 1.3.2 nor version 1.6.1.

Vulnerability Details

Alaris™ Gateway Workstation
BD has been made aware of a potential vulnerability that can impact the Workstation. If exploited, this vulnerability may allow an attacker with malicious intention to remotely install unauthorized firmware.

- In order to access this vulnerability, an attacker would need to gain access to a hospital network, have intimate knowledge of the product, be able to update and manipulate a CAB file, which stores files in an archived library and utilizes a proper format for Windows CE.
- If an attacker is able to complete those steps, they may also utilize this vulnerability to change the scope to adjust commands on the infusion pump, including adjust the infusion rate on specific mounted infusion pumps, listed above.
- In addition to the steps above, to exploit the vulnerability on the Workstation, an attacker would need to create an executable with custom code that can run in the Windows CE environment, understand how the internal communication protocols are utilized within the product and create a specific installer for the CAB file, with settings required to run the program.
- Adjusting the change in scope is difficult to exploit.

Alaris™ Gateway Workstation Web Browser User Interface
BD has been made aware of a potential vulnerability that can impact Web Browser User Interface on the Alaris Gateway Workstation, standalone configuration only. If exploited, this vulnerability may allow an attacker with knowledge of the IP address of the Alaris Gateway Workstation terminal to gain access to the following information on the Web Browser User Interface:

- Monitoring
- Event Logs
- User Guide
- Configuration

Note: Monitoring, Event Logs and User Guide have read-only access. Pages under configuration offer the ability to modify parameters.

- **By default, no patient information is stored on the Web Browser User Interface.**
- Additionally, an attack may be able to change the Workstation's network configuration and restart the Workstation. Pages under configuration include:
  - Identification
  - Date & Time; changes to these values would affect timestamps of log entries and snapshots of Patient Data Management System

- Alarm Settings
- Wired Networking
- Wireless Networking. This only applies to option 03 Workstations which utilize Wi-Fi adapters. This accounts for a small percentage of legacy devices.
- Serial ports

Select information may also be viewed as plain text through the portal.xml interface.

Clinical Risk Assessment and Patient Safety Impact

Alaris™ Gateway Workstation

- BD has assessed this with our clinical risk board and concluded that although the probability of remotely exploiting the vulnerability to the Workstation and then creating a custom, executable code that impacts the delivery of a patient's IV infusion is theoretically possible, the probability of patient harm is unlikely to occur due to the sequence of events that must occur in a specific order by a highly trained attacker.
- BD has had zero reports of this issue occurring from any customer sites.

Alaris™ Gateway Workstation Web Browser User Interface

- This vulnerability does not have a direct impact on any mounted infusion pump functionality or performance as this is a web-based application utilized for only the aggregation of data.

Mitigations & Compensating Controls

BD recommends the following mitigations and compensating controls in order to reduce risk associated with this vulnerability.

For the Alaris™ Gateway Workstation

- Users should utilize the latest firmware to eliminate the vulnerability
- BD recommends users block the SMB protocol
- Users should segregate their VLAN network
- Users should ensure only appropriate associates have access to the customer network

BD has created a remediation which removes accessibility to the SMB network share. Further details, including implementation of the remediation, will be provided on the BD Product Security website (https://www.bd.com/productsecurity) within 60 days of the original update, posted on June 13, 2019.

For the Alaris™ Gateway Workstation Web Browser User Interface

- BD recommends using the latest firmware version 1.3.2 or 1.6.1
- Users should ensure only appropriate associates have access to their network
- Users should isolate their network from untrusted systems

Further Information

The contents of this notification are disclosed publicly on the BD Product Security website (https://www.bd.com/productsecurity) and is voluntarily reported by BD to Information Sharing and Analysis Organizations (ISAOs) where BD participates, including the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the Health Information Sharing and Analysis Center (H-ISAC).
CyberMDX, a security vendor, originally made BD aware of these vulnerabilities to the Alaris™ Gateway Workstation and the Alaris™ Gateway Workstation Web Browser User Interface.

Customers should contact customer services as normal with any queries regarding specific customer site, implementation and remediation at 0800 917 8776.

Yours Sincerely,

Emma Stevens
Product Manager
MMS – Alaris™ Acute Pumps