Product Security Bulletin

Alaris™ Point of Care Unit (PCU)
Model 8015
October 2017

BD is committed to providing safe and secure products to our customers given the important benefits they provide to patient health. We value the confidentiality, integrity and availability of all protected health and personally identifiable information (e.g. PHI, PII) in accordance with all applicable federal and state privacy and security laws, including the Health Insurance Portability and Accountability Act.

This notification provides an update to the original disclosure posted in January 2017. It is intended to provide product security information and recommendations related to a security vulnerability found within certain versions of the Alaris™ Point of Care Unit (PCU) Model 8015.

Affected products

This notification applies to the following Alaris products:

- Alaris PCU Model 8015 9.5 and earlier. The Alaris PC unit software version 9.5 was released in 2010.
- Alaris PCU Model 8015 9.7 and later. The Alaris PC unit software version 9.7 was released in 2011.

Vulnerability Details

BD and independent security researchers have identified and confirmed a security vulnerability in certain older software versions of Alaris 8015 PCU that could allow an unauthorized user to access a facility's wireless network authentication credentials and other sensitive technical data by disassembling the Alaris PCU.

Vulnerable data may include:

- Wireless network Service Set Identifier (SSID)
- Wired Equivalent Privacy (WEP) keys
- WiFi Protected Access (WPA) Username, Password, Passphrase
- Root/Client Certificates
- Advanced Encryption Standard (AES) keys used to encrypt data in transit
- Alaris Systems Manager internet protocol (IP) address
- Operating System Components and Interfaces that may impact the integrity of device operations

Depending on current software version and PCU Revision, these components may be accessed differently.

BD also discovered that a limited set of ePHI elements could potentially be accessed when an unauthorized user disassembles the Alaris 8015. The limited set of ePHI elements may include:

- Patient ID
- Infusion parameters
- Past infusion history
- Patient weight (for weight based infusion)

Please note that the above mentioned ePHI elements do not uniquely identify an individual.

Alaris PCU model 8015 with software version 9.5 or earlier

BD and independent security researchers have identified a security vulnerability in older software versions of the Alaris PCU model 8015 which could allow an attacker with physical access to an Alaris PCU device to obtain unencrypted wireless network authentication credentials and other sensitive technical data by disassembling the Alaris PCU and accessing the device's removable flash memory.

For an attacker to exploit this vulnerability, an attacker must physically disassemble the Alaris PCU model 8015 to remove the CompactFlash memory card and use a computer to access the card contents.

Alaris PCU model 8015 with software version 9.7 or later

Software versions 9.7 and later do not store any credentials on the removable CompactFlash memory card but instead store this data on internal flash memory.

For an attacker to exploit this vulnerability, an attacker must physically disassemble the Alaris PCU model 8015 to access the circuit boards containing the flash memory chip. The attacker would then have to perform one of two potential attacks to read the sensitive data:

1. Obtain knowledge of the Alaris command interface and craft a script to copy credentials

2. Use advanced tools to read the flash memory, decode the file system, and finally locate and read the sensitive data

To date there have been no reports of this vulnerability being exploited but the vulnerability has been confirmed.

Clinical Risk Assessment and Patient Safety Impact

This vulnerability has been assessed for clinical impact by BD and represents little to no risk to patient safety, since no modifications can be made remotely to the clinical functions of the Alaris PCU.

Product Security Risk Assessment and Vulnerability Score

BD has conducted internal risk assessments for this vulnerability and has also collaborated with the U.S. Department of Homeland Security (DHS), Food and Drug Administration (FDA), and independent security researchers to review baseline Common Vulnerability Scoring

System (CVSS) scores as outlined below. These vulnerability scores can be used in assessing risk within your own organization.

8015 with software version 9.5 or earlier:
6.8 (MED) CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Rationale: Physical access is required to exploit this vulnerability. Attack complexity is LOW based on availability of these wireless credentials on the PCU removable Flash card, and no system privilege is required. The scope is considered unchanged as the disclosure of a password is a loss of confidentiality on the local system and subsequent attacks would be necessary to change scope. The Network credentials are considered sensitive parameters which results in the Confidentiality impact as HIGH.

8015 with software version 9.7 or later:
4.9 (MED) CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N

Rationale: Physical access is required to exploit this vulnerability. Attack complexity is HIGH based on availability of the command interface to obtain the wireless credentials which are stored in the PCU on internal flash memory. The attacker would have to obtain knowledge of the command interface used by the Alaris PCU. No system privilege is required.
The scope is considered unchanged as the disclosure of wireless credentials stored in the PCU's internal flash memory is a loss of confidentiality. The Network credentials are considered sensitive parameters which results in the Confidentiality impact as HIGH.

Mitigations & Compensating Controls

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

- It is recommended that Alaris PCU model 8015 customers upgrade from software version 9.5 to the latest Alaris PCU software in order to further mitigate associated risks.

- Customers are advised to follow procedures for clearing wireless network authentication credentials on the Alaris PCU if the device is to be removed from service or it will not be in control of institutional staff. These procedures are outlined in the Alaris System Maintenance Software User Manual, page 13. Properly clearing wireless network authentication credentials is recommended when emergency patient transport is imminent, or when a device may be out of staff control.

- Customers are advised to change their wireless network authentication credentials regularly, and immediately if there is evidence of unauthorized physical access to an Alaris device at their facility. Additionally, all wireless credentials should be cleared prior to transferring an Alaris device to another facility. Where feasible, customers are encouraged to utilize enterprise-grade authentication methods, e.g. EAP-TLS.

- Customers are strongly encouraged to consider security policy in which wireless credentials are not configured for the Alaris PCU if wireless networking functionality is not being utilized for operation. This will remediate the vulnerability for non-wireless users.

- Customers are advised to implement a policy of using tamper-evident seals on the rear access panel and on the grooves of both sides of the Alaris PCU.

- Customer may choose to implement Access Control Lists (ACLs) that restrict device access to specific media access control (MAC) and IP addresses, ports, protocols, and services.

For More Information

For more information on BD's proactive approach to product security and vulnerability management contact BD Product Security:

http://www.bd.com/aboutbd/productsecurity/

BD
San Diego, CA
United States 888.876.4287
858.617.2000
bd.com