Product Security Bulletin

Alaris™ PC Unit (PCU)
Model 8015
January 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 product security information and recommendations related to a security vulnerability found within certain versions of the Alaris™ PCU model 8015.

Affected products

This notification applies to the following Alaris products:

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

Vulnerability Details

BD and independent security researchers have identified a security vulnerability in certain 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.

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

Depending on current software version, this data may be accessed differently.

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 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 open the Alaris PCU model 8015, which would allow access to the CompactFlash memory card that could then be removed and accessed using a computer.
This vulnerability has been successfully demonstrated to BD.

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 open the Alaris PCU model 8015, which would allow access to circuit boards containing the flash memory chip. The attacker would then have to use advanced tools to read the flash memory, decode the file system, locate and read the credential data.

To date there have been no reports of this vulnerability being exploited.

Clinical Risk Assessment and Patient Safety Impact

This vulnerability has been assessed for clinical impact by BD and represents a negligible probability of harm to the patient, 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), U.S. Food and Drug Administration (FDA), and independent security researchers to review baseline and temporal 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:
5.3 (MED) CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

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. Due to the Changed Scope element of this vulnerability and the nature of data that could be accessed (local wireless network access/authentication credentials and other info discussed as Vulnerable Data), Confidentiality impact is 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 limited availability of these wireless credentials that are stored in the PCU on internal flash memory. The attacker would then have to use advanced tools to read the flash memory, decode the file system, and then locate and read the credential data. No system privilege is required. Due to the Changed Scope element of this vulnerability with regards to wireless network access credentials, Confidentiality impact is 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 or transported from the facility. These procedures are outlined in the Alaris System Maintenance Software User Manual.

- 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.

- 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.

- For Alaris PCU model 8015 devices version 9.7 and later, BD has implemented Federal Information Processing Standard (FIPS) 140-2 Level 2 physical security controls, including standard tamper-evident physical seals which can be applied to hardware to provide indication of unauthorized physical access.

  Customers should review "FIPS 140-2 Compliance Instructions for Alaris Products" guide, pages 11-29, for information on how to enforce FIPS 140-2 level 2 physical security controls on the Alaris PC unit.

- Customers 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.

- A customer may choose to place Alaris PCUs on an isolated network with dedicated SSID to reduce the impact of compromised wireless network credentials. In all cases, security best practice prescribes frequent changing of SSID and wireless authentication credentials.

For More Information

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

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

Product Security Bulletin

Alaris™ PC Unit (PCU)
Model 8015
January 2017

January 2017
Product Security Bulletin for Alaris PCU model 8015

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