Product Security Bulletin
Alaris^{TM} PC Unit (PCU)
Model 8000
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 specified versions of Alaris^{TM} PC Unit Model 8000.

Affected products

This notification applies to the following Alaris products:

- Alaris PCU Model 8000 (all software versions)

Vulnerability Details

BD and independent security researchers have identified a security vulnerability in specified Alaris PCU model 8000 that could allow an attacker with physical access to a PCU device to obtain unencrypted wireless network authentication credentials and other sensitive technical data by disassembling the PCU and accessing the device's flash memory.

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

Alaris PCU model 8000 (all software versions)

For an attacker to exploit this vulnerability, an attacker must physically open the Alaris PCU model 8000 and read contents of the onboard flash memory using a specialized tool. To date there have been no reports of this vulnerability being exploited on the Alaris PCU model 8000.

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), the 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.

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 and an attacker would be able to read the credential data without a user name or password. 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**.**

Mitigations & Compensating Controls

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

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

- Customers are advised to change their wireless network authentication credentials if there is evidence of unauthorized physical access to an Alaris PCU at their facility.

- 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.

- 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
January 2017
Product Security Bulletin for Alaris PCU model 8000

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