Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Advisory (ICSA-15-125-01)

More Advisories

Hospira LifeCare PCA Infusion System Vulnerabilities

Original release date: May 05, 2015

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Independent researcher Billy Rios has identified an improper authorization vulnerability and an insufficient verification of data authenticity vulnerability in Hospira's LifeCare PCA Infusion System, which NCCIC/ICS-CERT has been coordinating with Hospira since May 2014. This advisory is being issued to provide notice of public disclosures of the identified vulnerabilities in the LifeCare PCA Infusion System. Hospira has developed a new version that mitigates these vulnerabilities, which is undergoing U.S. Food and Drug Administration (FDA) review. The release date for the new version has not been determined.

These vulnerabilities could be exploited remotely.

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

AFFECTED PRODUCTS

The following Hospira products are affected:

- LifeCare PCA Infusion System, Version 5.0 and prior versions.

IMPACT

Exploitation of the improper authorization vulnerability may allow unauthenticated users to access the LifeCare PCA Infusion pump with root privileges by default. Exploitation of the insufficient verification of data authenticity vulnerability may allow an attacker to remotely push unauthorized modifications to the LifeCare PCA Infusion pump impacting medication libraries and pump configuration. While drug libraries, software updates, and pump configurations can be modified, according to Hospira, it is not possible to remotely operate the LifeCare PCA Infusion pump. Operation of the LifeCare PCA Infusion pump requires a clinician to be present at the pump to manually program the pump with a specified dosage before medication can be administered.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Hospira is a US-based company that maintains offices in several countries around the world.

The affected product, the LifeCare PCA Infusion System, is an intravenous pump that delivers medication to patients. The affected products are deployed across the Healthcare and Public Health Sector. Hospira estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER AUTHORIZATION[a]

The LifeCare PCA Infusion pump's communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user may be able to issue commands to modify the configuration of the pump.

CVE-2015-3459[b] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[c]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[d]

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

The LifeCare PCA Infusion pump could have drug libraries, software updates, and configuration changes uploaded to it from an unauthorized source. The LifeCare PCA Infusion pump listens on the following ports: Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP.

CVE-2014-5406[e] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with low skill would be able to exploit one of these vulnerabilities; the other vulnerability would require high skill to exploit.

MITIGATION

ICS-CERT has been working with Hospira since May 2014 to address the vulnerabilities in the LifeCare PCA Infusion System. Hospira has developed a new version of the PCS Infusion System, Version 7.0 that addresses the identified vulnerabilities. According to Hospira, Version 7.0 has Port 20/FTP and Port 23/TELNET closed by default to prevent unauthorized access. Existing PCA Infusion Systems running Version 5.0 can be upgraded to Version 7.0 when it becomes available. Hospira's Version 7.0 is being reviewed by the FDA prior to its release. The release date for Version 7.0 of the LifeCare PCA Infusion System has not been determined.

For additional information about Hospira's new release, contact Hospira's technical support at 1 800-241-4002.

ICS-CERT encourages asset owners to take defensive measures to protect against this and other cybersecurity risks.

- Ensure that unused ports are closed, to include Port 20/FTP and Port 23/TELNET.
- Maintain layered physical and logical security to implement defense-in-depth security practices for environments operating medical devices.
- Isolate the LifeCare PCA Infusion pump from the Internet and untrusted systems; however, if connectivity is required, use a Virtual Private Network (VPN) solution and implement network monitoring.
- When remote access is required, use secure methods, such as VPNs, recognizing that VPNs may have

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

- Produce an MD5 checksum of key files to identify any unauthorized changes.
- Use good design practices that include network segmentation. Use DMZs with properly configured firewalls to selectively control traffic and monitor traffic passed between zones and systems to identify anomalous activity. Use the static nature of these isolated environments to look for anomalous activities.

ICS-CERT also provides a section for security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

---

a. CWE-285: Improper Authorization, http://cwe.mitre.org/data/definitions/285.html, web site last accessed May 05, 2015.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3459, web site last accessed May 05, 2015.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C, web site last accessed May 05, 2015.

d. CWE-345: Insufficient Verification of Data Authenticity, http://cwe.mitre.org/data/definitions/345.html, web site last accessed May 05, 2015.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5406, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:H/Au:N/C:C/I:C/A:C, web site last accessed May 05, 2015.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

Was this document helpful? Yes | Somewhat | No

I Want To

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about Reporting

Join the Secure Portal

ICS-CERT encourages U.S. asset owners and operators to join the Control Systems compartment of the US-CERT secure portal. Send your name, e-mail address, and company affiliation to ics-cert@hq.dhs.gov.

Mailing Lists and Feeds **Follow ICS-CERT on Twitter**

Contact Us

(877) 776-7585
(208) 526-0900
(International Callers)

ICS-Related Cyber Activity

General ICS Questions

Download PGP/GPG keys

US-CERT is part of the Department of Homeland Security.

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com