Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Search

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems

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

More Advisories

Advisory (ICSA-15-161-01)

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 11, 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 vulnerabilities in Hospira's Plum A+ Infusion System that are similar to vulnerabilities identified in Hospira's LifeCare PCA Infusion System discussed in advisory, ICSA-15-125-01B Hospira LifeCare PCA Infusion System Vulnerabilities. Hospira identified vulnerabilities in the Symbiq Infusion System. Kyle Kamke of Ramparts, LLC has identified an uncontrolled resource consumption vulnerability in Hospira's Symbiq Infusion System. NCCIC/ICS-CERT is reporting on these vulnerabilities to notify healthcare providers of a coordinated disclosure of vulnerability information and to provide additional defensive measures to help mitigate risks associated with these vulnerabilities. Hospira is releasing the Plum 360 Infusion System, a new version of Plum A+.

These vulnerabilities could be exploited remotely. Exploits that target some of these vulnerabilities are known to be publicly available.

AFFECTED PRODUCTS

The following Hospira products are affected:

- Plum A+ Infusion System, Version 13.4 and prior versions,
- Plum A+3 Infusion System, Version 13.6 and prior versions, and
- Symbiq Infusion System,[a] Version 3.13 and prior versions.

IMPACT

Successful exploitation of these vulnerabilities, in a worst case scenario, may allow an attacker to impact the core functions of the device.

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 products, the Plum A+ Infusion System (which includes Plum A+ and the Plum A+3 Infusion System), are intravenous pumps that deliver 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

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] 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).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] 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).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP.

CVE-2015-3956[i] 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).[j]

USE OF HARD-CODED PASSWORD[k]

Hard-coded accounts may be used to access the device.

CVE-2015-3953[l] 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).[m]

CLEARTEXT STORAGE OF SENSITIVE INFORMATION[n]

Wireless keys are stored in plain text on the device.

CVE-2015-3952[o] has been assigned to this vulnerability. A CVSS v2 base score of 6.4 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:N).[p]

KEY MANAGEMENT ERRORS[q]

Private keys and certificates are stored on the device.

CVE-2015-3957[r] has been assigned to this vulnerability. A CVSS v2 base score of 4.6 has been assigned; the CVSS vector string is (AV:L/AC:L/Au:N/C:P/I:P/A:P).[s]

VULNERABLE SOFTWARE VERSION USED

The web server is reportedly running vulnerable versions of AppWeb, to include Versions 1.0.2, which contain numerous vulnerabilities. The Plum A+ Infusion System, versions prior to, but not including Version 13.4 and the Plum A+3 Infusion System, versions prior to, but not including Version 13.6 are affected. The Symbiq Infusion System, versions prior to, but not including Version 3.0 are affected.

UNCONTROLLED RESOURCE CONSUMPTION[t]

The device is susceptible to a denial-of-service condition as a result of an overflow of TCP packets, which requires the device to be manually rebooted.

CVE-2015-3958[u] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[v]

VULNERABILITY DETAILS

EXPLOITABILITY

All but one of these vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target some of these vulnerabilities are known to be publicly available.

DIFFICULTY

An attacker with low skill would be able to exploit all but two of these vulnerabilities; the remaining vulnerabilities would require high skill to exploit.

MITIGATION

Hospira is communicating with customers to direct them to close Port 20/FTP and Port 23/TELNET on the affected devices. In addition, Hospira is also releasing its Plum 360 Infusion System. Hospira asserts that the Plum 360 uses a different architecture than the Plum A+ Infusion System and is not vulnerable to the reported vulnerabilities.

For additional information about the vulnerabilities and compensating measures, contact Hospira's technical support at 1-800-241-4002.

ICS-CERT strongly encourages asset owners to perform a risk assessment by examining their specific clinical use of the affected products in their host environment to identify any potential impacts of the identified vulnerabilities. ICS-CERT offers the following compensating options:

- Temporarily disconnect the affected product from the wireless network until unused ports on the device are closed, to include Port 20/FTP and Port 23/TELNET. Once the unused ports have been closed, reconnecting the affected device to the wireless network should be done after ensuring that the host network is isolated from the Internet. The affected product should be isolated from untrusted systems; traffic to the device should be selectively controlled and monitored for anomalous activity.
- Disconnect the affected product from the wireless network and use a wired connection to the host network. The operational concerns associated with this option are primarily associated with the initial setup of the wired connection and verifying that the host network effectively implements good design practices prior to connection of the affected product.
- If neither of the previous two options are feasible, then disconnect the affected product from the wireless network until mitigations are available. Disconnecting the affected product from the wireless network will have operational impacts. Disconnecting the device will require drug libraries to be updated manually and data normally transmitted to MedNet from the device, will not be available. Manual updates to each pump can be labor intensive and prone to entry error.

ICS-CERT encourages asset owners to implement the following defensive measures to protect against this and other cybersecurity risks. Specifically, users should:

- **Ensure that unused ports are closed, to include Port 20/FTP and Port 23/TELNET.**
- Hospira strongly recommends that healthcare providers change the default password used to access Port 8443.
- Monitor and log all network traffic attempting to reach the affected product via Port 20/FTP, Port 23/TELNET and Port 8443.
- 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.
- Maintain layered physical and logical security to implement defense-in-depth security practices for environments operating medical devices.
- Isolate all medical devices from the Internet and untrusted systems.
- Produce an MD5 checksum of key files to identify any unauthorized changes.

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] As previously announced by Hospira in 2013, the Symbiq Infusion System was retired by Hospira on May 31, 2015 and will be fully removed from the market by December 2015. According to Hospira, during a recent service visit, the remaining Symbiq Infusion Systems have had Port 20/FTP and Port 23/TELNET closed.

[b] CWE-121: Stack-based Buffer Overflow, http://cwe.mitre.org/data/definitions/121.html, web site last accessed June 10, 2015.

[c] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3955, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

[d] 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 June 10, 2015.

[e] CWE-285: Improper Authorization, http://cwe.mitre.org/data/definitions/285.html, web site last accessed June 10, 2015.

[f] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3954, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

g. 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 June 10, 2015.

h. CWE-345: Insufficient Verification of Data Authenticity, http://cwe.mitre.org/data/definitions/345.html, web site last accessed June 10, 2015.

i. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3956, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

j. 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 June 10, 2015.

k. CWE-259: Use of Hard-coded Password, http://cwe.mitre.org/data/definitions/259.html, web site last accessed June 10, 2015.

l. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3953, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

m. 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 June 10, 2015.

n. CWE-312: Cleartext Storage of Sensitive Information, http://cwe.mitre.org/data/definitions/312.html, web site last accessed June 10, 2015.

o. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3952, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

p. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:P/I:P/A:N, web site last accessed June 10, 2015.

q. CWE-320: Key Management Errors, http://cwe.mitre.org/data/definitions/320.html, web site last accessed June 10, 2015.

r. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3957, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

s. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:L/AC:L/Au:N/C:P/I:P/A:P, web site last accessed June 10, 2015.

t. CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion'), http://cwe.mitre.org/data/definitions/400.html, web site last accessed June 10, 2015.

u. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3958, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

v. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C, web site last accessed June 10, 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

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

Home | FAQ | Traffic Light Protocol | Privacy & Use | Accessibility | Get a PDF Reader

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