2014/4/21

To: Itron Customers

From: Itron CTO Security Team

Re: Heartbleed Vulnerability

Many customers have inquired about the potential vulnerability of Itron products in regards to Heartbleed (CVE-2014-0160), a security bug in the open-source OpenSSL cryptography library. Details on the Heartbleed vulnerability can be found at http://heartbleed.com.

Itron is committed to the security of products. We have reviewed our product portfolio to determine whether our products are vulnerable to this attack. Itron uses a variety of cryptographic libraries to provide encryption services to protect our products, including technology from Microsoft, RSA and Certicom. Most Itron products do not use OpenSSL, and as a result are not vulnerable to this attack. Software products that do not use OpenSSL include:

- Distribution Design Studio
- Eclipse Enterprise Edition
- Eclipse Vendor Gateway
- EMMSYS
- Field Collection System
- Field Deployment Manager
- Fixed Network NCE (4.x and higher)
- Frontline
- Itron Business Analytics
- Itron Enterprise Edition
- Itron Security Manager
- MV-90 xi
- MVLT xi
- MV-PBS
- MV-RS
- MV-Web
- OpenWay Collection Engine
- OpenWay Reporting System
- Saturne
- Saturne AMS
- Talexus
- TMS

ITRON
2111 North Molter Road
Liberty Lake, WA 99019
www.itron.com

Hardware products that do not use OpenSSL include:

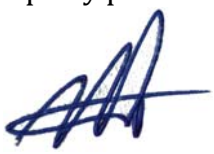
- ACE4K PxMM Meter
- ACE6K Meter
- ACE8K Meter
- Choice Connect ERT Modules (All available variants)
- CENTRON Meter (All available variants)
- FC300
- Galvani Meter
- Itron Adaptive Grid Router
- Itron Cellular Module (Generation 1) A3
- Itron Cellular Module (Generation 1) A3 Collector
- Itron Cellular Module (Generation 1) CENTRON
- Itron Cellular Module (Generation 1) I210C
- Itron Cellular Module (Generation 1) KV2C
- Itron Cellular Module (Generation 1) OpenWay CENTRON
- Itron Cellular Module (Generation 1) SENTINEL
- Linky Meter
- Mobile Collector
- Mobile Collector Lite
- OpenWay CENTRON Meter (All available variants)
- OpenWay Certicom Security Appliances
- OpenWay Tropos Mesh Router
- SL7K Meter
- T5 Meter

The Itron products listed below do use OpenSSL. We have reviewed these products and determined that they are not vulnerable because they use versions of OpenSSL that do not contain the vulnerability:

- Itron Cellular Module (Generation 2) I210C
- Itron Cellular Module (Generation 2) KV2C
- Itron Cellular Module (Generation 2) CENTRON
- CCU 4.2, 5.1, 100
- Fixed Network NCE (3.x)

Itron produces a wide-variety of products. If you have questions about an Itron product not listed here, please contact your Itron representative or the Itron CTO Security team (secure@itron.com).

Please note that Itron products are typically deployed in a larger context. While these Itron products are not vulnerable, third party tools used with them may be. We encourage our customers to evaluate their entire deployment and reach out to third party providers if there are concerns.



Michael Garrison Stuber
Itron CTO Security Team