2014/11/11

To: Itron Customers
From: Itron CTO Security Team
Re: Bash ("Shellshock") Vulnerability

On Wednesday, September 24, a vulnerability in the bash command shell was publically disclosed. Command shells are programs used in Linux, Unix and similar operating systems to execute commands. "Bash" is one of several command shells available, but it is widely used as the default command shell for Linux operating systems. Command shells are a core part of these operating systems and are often used when one program executes another. As a result, this vulnerability may be exploitable remotely over a network connection.† This vulnerability has been assigned CVE-2014-6271 and CVE-2014-7169. More details can be found at https://shellshocker.net.

Itron is committed to the security of our products. We have reviewed our product portfolio to determine whether our products are vulnerable to this attack. Itron uses a variety of different operating systems with our products. Most Itron software products are Microsoft Windows™ based, and, as a result, are not vulnerable to this attack. This includes:

- Distribution Design Studio
- Eclipse Enterprise Edition
- Eclipse Vendor Gateway
- EMMSYS
- Field Collection System
- Field Deployment Manager
- Fixed Network NCE
- Frontline
- Itron Adaptive Grid Router
- 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

† The vulnerability allows an attacker to use environmental variables to submit arbitrary commands for execution. One method of remote attack is to submit a specially formed request to a web server which uses Common Gateway Interface (CGI) scripts. An example can be found at http://security.stackexchange.com/questions/68122/what-is-a-specific-example-of-how-the-shellshock-bash-bug-could-be-exploited. Another method of remote attack is to submit tainted environmental variables via Dynamic Host Configuration Protocol (DHCP). See https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept.

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

Most Itron hardware products use specialized embedded operating systems known as micro-kernels and do not include any sort of command shell. Some Itron hardware products use Microsoft Windows-CE or use embedded Linux, but do not use the bash shell. These products are not vulnerable to this attack. This includes:

- ACE4K PxMM Meter
- ACE6K Meter
- ACE8K Meter
- Choice Connect ERT Modules (All available variants)
- Cisco Connected Grid Router‡
- Cisco Connected Grid Network‡ Management System
- CENTRON Meter (All available variants)
- FC300 Handheld
- Galvani Meter
- Itron Cellular Module (All available variants)
- Linky Meter
- Mobile Collector
- Mobile Collector Lite
- OpenWay CENTRON Meter (All available variants)
- OpenWay Cell Relay (All available variants)
- SL7K Meter
- T5 Meter

Some products produced by Itron and our partners use the vulnerable version of Bash. While these products are vulnerable, none of them are directly exploitable under normal deployment conditions. In the case of third party products, we encourage affected customers to contact these providers directly. Vulnerable products include:

- Itron Choice Connect CCU 4.x, 5.x, & 100
  These products are vulnerable; however, this vulnerability is not exposed externally. An attacker would need login access to the CCU to exploit this vulnerability. Itron does not currently have a patch available.
- Lockheed Martin Industrial Defender Security Event Manager
  Lockheed Martin has indicated that the Industrial Defender Security Event Manager is vulnerable, but this vulnerability is not directly exposed, so it is not readily exploitable. Lockheed Martin will be issuing a patch. Users are encouraged to go to https://support.industrialdefender.com/ or contact support@industrialdefender.com
- OpenWay Certicom Security Appliances
  Certicom has indicated that the Linux operating system used in the Certicom Security Appliances is vulnerable, but this vulnerability is not directly exposed by the appliances, so it is not readily exploitable. Certicom will be providing patch procedures to customers.
- OpenWay Tropos Mesh Router & OpenWay Control
  ABB has indicated that most Tropos Mesh Routers are vulnerable, but this vulnerability is not directly exposed, so it is not readily exploitable. ABB will

‡ See Cisco's Bash security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash

be issuing a patch for the Tropos Mesh Routers. OpenWay Control does not use BASH, but it relies on the Linux Operating System which does. Users are encouraged to patch their operating systems. Details can be found at https://www.tropos.com/pv/1KHA001368_ABB_SoftwareVulnerabilityHandlingAdvisory_ABB-VU-PSNM-15473.pdf

Itron will provide updated information as soon as it becomes available. New versions of this letter will be posted to http://www.itron.com/security as additional information becomes available. Please note that CCUs, mesh routers, and the OpenWay security appliances are typically deployed in isolated network environments which minimize any opportunity for attack.

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).

Itron products are 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