Server Technology, Inc.

1040 Sandhill Drive
Reno, Nevada 89521

www.servertech.com
+1.775.284.2000
+1.800.835.1515
+1.775.284.2065

September 30, 2014 **UPDATE 1**

Subject: Shellshock Threat / CVE-2014-6271/6277/6278/7169/7186/7187 (Bash version 4.1-2ubuntu3.4)

Products: All Server Technology CDU's and SPM (Sentry Power Manager)

Vulnerability Summary: The bug, discovered by Stephane Schazelas, is related to how Bash processes environmental variables passed by the operating system or by a program calling a Bash-based script. If Bash has been configured as the default system shell, it can be used by network–based attackers against servers and other Unix and Linux devices via Web requests, secure shell, telnet sessions, or other programs that use Bash to execute scripts.

Server Technology CDU's:

Server Technology CDU's are NOT vulnerable to the Bash "Shellshock" vulnerability.

The Bash "Shellshock" vulnerability relies upon the exploit of a flaw in the Bash shell of Linux, Unix, and Mac OS X platforms. Server Technology CDUs use Digi International's NET+OS 7 Integrated Real-Time OS platform that is based on the ThreadX Real-Time Operating System by Express Logic. NET+OS has no support for a Bash shell. As such, NET+OS is completely unaffected by the Bash "Shellshock" vulnerability.

Server Technology SPM System:

SPM does not use bash as the default shell. We use a custom SPM written shell for items like telnet, SSH, ftp, console and serial connections. As an appliance we also block access to the root shell. We do use bash for our internal scripts and these are under our control.

Though other concerns related to this threat mention both Apache and DHCP and could possibly make us vulnerable.

Solution:

To be safe a patch is available for SPM versions 5.3 or 5.4. Please contact STI Support.

To Contact STI Support:

Phone: (01) 800-835-1515
Email: support@servertech.com