EndRun
TECHNOLOGIES

2270 Northpoint Parkway, Santa Rosa, CA 95407

FIELD SERVICE BULLETIN

FSB# 140926-03
September 26, 2014

Affected Products:

All products listed below.

Part Number:	**Description:**
3003-00xx-00x	Praecis Cntp Network Time Server
3005-00xx-00x	Praecis Gntp Network Time Server
3007-xxxx-00x	Praecis Cntp Network Time Server
3009-00xx-00x	Praecis Gntp Network Time Server
3012-00xx-00x	Tempus Gntp Network Time Server
3013-00xx-00x	Tempus Cntp Network Time Server

Note: “x” is variable.

Problem:

Shellshock vulnerability CVE-2014-6271

Vulnerability detected in the Linux operating system `bash` shell. If you have NOT secured your Time Server according to best practices, then it might allow remote attackers to execute code. Details are here:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

Required Action:

Your Time Server is secure as long as you have properly restricted access control. If you haven't already done so, then please perform the following steps:

1. Disable TELNET which has always been insecure. Use the `inetdconfig` command which is described in your ***User Manual, Control and Status Commands, inetdconfig***. Links to the user manuals are listed below.

2. Configure *hosts.allow/hosts.deny* to limit SSH login access to specific hosts. Read about the `accessconfig` command in your ***User Manual, Security Appendix***. Links to the user manuals are listed below.

3. Disable login access for ALL non-administrative users by changing the unprivileged user password. To do this, at the command line interface type the following command (depending on your product):

Praecis Gntp & Tempus Gntp	**gntppasswd gntpuser**
Praecis Cntp & Tempus Cntp	**cntppasswd cntpuser**

Background Information:

The ShellShock vulnerability is only a threat to your Time Server if it is NOT being managed according to recommended best practices for access control. It is only possible to exercise the threat by an authenticated user, or via DHCP from a malicious DHCP server, such as from a public internet access point.

EndRun networked products have always employed a minimalist suite of protocols--only those necessary for the specific function the appliances provide. By disabling those that are not essential, the security risks are minimized. Since the products are not general-use servers, login access should be restricted to a handful of adminstrative personnel from a handful of specific hosts. We believe that restricting access will eliminate the risks presented by the ShellShock vulnerability and most future vulnerabilites as well.

The following paper describes recommended best practices for our Sonoma Time Server, but in general, the recommendations are the same for your Time Server:
http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

User Manuals:

Praecis Cntp	http://www.endruntechnologies.com/pdf/cntpmanual.pdf
Praecis Gnp	http://www.endruntechnologies.com/pdf/gntpmanual.pdf
Tempus Cntp	http://www.endruntechnologies.com/pdf/TempusCntpManual.pdf
Tempus Gntp	http://www.endruntechnologies.com/pdf/TempusGntpManual.pdf

Contact Information:

Feel free to contact us if you have any questions or need help:

EndRun Technologies
2270 Northpoint Parkway
Santa Rosa, CA 95407
USA
707-573-8633 or 1-877-749-3878 (toll-free in the USA & Canada)
support@endruntechnologies.com