EndRun
TECHNOLOGIES

2270 Northpoint Parkway, Santa Rosa, CA 95407

FIELD SERVICE BULLETIN

FSB# 140926-02
September 26, 2014
(Revised October 17, 2014)

Affected Products:

All products listed below.

Part Number:	**Description:**
3014-00xx-00x	Tempus LX CDMA Network Time Server
3015-00xx-00x	Tempus LX GPS Network Time Server
3016-00xx-00x	Unison CDMA Network Time Server
3017-00xx-00x	Unison GPS Network Time Server
3018-00xx-00x	Tempus LX CDMA Network Time Server (Japan)
3020-xxxx-00x	Tycho CDMA Frequency Reference
3021-xxxx-00x	Tycho GPS Frequency Reference
3019-xxxx-00x	Meridian Precision GPS TimeBase
3025-xxxx-00x	Meridian CDMA Frequency Reference

Note: “x” is variable.

Problem:

Shellshock vulnerabilities CVE-2014-6271, -6277, -6278, -7169

Vulnerabilities have been detected in the Linux operating system **bash** shell. If you have the Web Interface (HTTP) enabled on your Time Server, or 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
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

Required Action:

Firmware is available that eliminates the Shellshock vulnerabilities listed above. Go to one of the following links for the Linux Subsystem firmware with upgrade instructions:

Tempus LX (GPS & CDMA)	http://www.endruntechnologies.com/upgradetemplx.htm
Unison (GPS & CDMA)	http://www.endruntechnologies.com/upgradeuni.htm
Meridian (GPS)	http://www.endruntechnologies.com/upgrademer.htm
Meridian (CDMA)	http://www.endruntechnologies.com/upgrademerC.htm
Tycho (GPS & CDMA)	http://www.endruntechnologies.com/upgradetyc.htm

Or... if you do not want to upgrade firmware at this time, then disable the Web Interface (HTTP) and follow best practices for access control. This will protect your Time Server from the Shellshock threat. To properly control access, perform the steps below:

1. If you have the Web Interface enabled, then see your ***User Manual, Appendix A – Security, Disable SNMP and HTTP*** for instructions on how to disable it. Links to the user manuals are listed below. ‘

2. Disable TELNET which has always been insecure. See your ***User Manual, Appendix A – Security, Disable Telnet, TIME and DAYTIME***. Links to the user manuals are listed below.

3. Configure *hosts.allow/hosts.deny* to limit SSH login access to specific hosts. See your ***User Manual, Appendix A – Security, Limiting Access*** for details. Links to the user manuals are listed below.

4. Disable login access for ALL non-administrative users by changing the unprivileged user password. To do this, at the command line interface, type one of the following commands:

Tempus LX (GPS) & Unison (GPS)	**`gntppasswd gntpuser`**
Tempus LX (CDMA) & Unison (CDMA)	**`cntppasswd cntpuser`**
Meridian (GPS) & Tycho (GPS)	**`gsyspasswd gsysuser`**
Meridian (CDMA) & Tycho (CDMA)	**`csyspasswd csysuser`**

Background Information:

The ShellShock vulnerabilities are only a threat to your EndRun product if the Web Interface (HTTP) is enabled and you are NOT managing the unit according to recommended best practices for access control. Otherwise, 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 EndRun product:
http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

User Manuals:

Tempus LX (CDMA)	http://www.endruntechnologies.com/pdf/USM3014-0000-000.pdf
Tempux LX (GPS)	http://www.endruntechnologies.com/pdf/USM3015-0000-000.pdf
Unison (CDMA)	http://www.endruntechnologies.com/pdf/USM3016-0000-000.pdf
Unison (GPS)	http://www.endruntechnologies.com/pdf/USM3017-0000-000.pdf
Tycho (CDMA)	http://www.endruntechnologies.com/pdf/USM3020-0000-000.pdf
Tycho (GPS)	http://www.endruntechnologies.com/pdf/USM3021-0000-000.pdf
Meridian (CDMA)	http://www.endruntechnologies.com/pdf/USM3025-0000-000.pdf
Meridian (GPS)	http://www.endruntechnologies.com/pdf/USM3019-0000-000.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