

FIELD SERVICE BULLETIN

FSB# 151026
October 26, 2015

Affected Products:

Sonoma, Meridian II, Tycho II, Tempus LX, Unison, Meridian

Part Number:	Description:
3014-xxxx-xxx	Tempus LX CDMA Network Time Server
3015-xxxx-xxx	Tempus LX GPS Network Time Server
3016-xxxx-xxx	Unison CDMA Network Time Server
3017-xxxx-xxx	Unison GPS Network Time Server
3018-xxxx-xxx	Tempus LX CDMA Network Time Server (Japan)
3019-xxxx-xxx	Meridian Precision GPS TimeBase
3025-xxxx-xxx	Meridian CDMA Frequency Reference
3026-xxxx-xxx	Sonoma D12 Network Time Server (CDMA)
3027-xxxx-xxx	Sonoma D12 Network Time Server (GPS)
3028-xxxx-xxx	Sonoma N12 Network Time Server (CDMA)
3029-xxxx-xxx	Sonoma N12 Network Time Server (GPS)

Note: "x" is variable.

Problems:

Vulnerabilities announced in the October 2015 NTP Security Vulnerability Announcement

Details are at ntp.org here: [October 2015 Security Vulnerability Announcement](#)

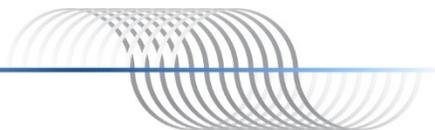
As described at the link above, a list of low- and medium-severity vulnerabilities were fixed in the latest *ntpd* version 4.2.8p4. Since the impact to EndRun's products is very limited and easily mitigated, there will be no immediate firmware release to incorporate 4.2.8p4.

Required Action:

EndRun's NTP Servers with the latest firmware and factory-default configuration settings in the *ntp.conf* file are NOT susceptible to these vulnerabilities. Your NTP Server is only vulnerable if you have changed the configuration to permit peering or Stratum 2 operation. We have always recommended against peering as explained here: [About Peering and Stratum 2](#).

These vulnerabilities are more of a concern for your NTP [clients](#). After updating your clients to the latest *ntpd* version 4.2.8p4, you should use MD5 authentication as described in the *Use Authentication* section here: [Best Practices to Secure Your Time Server](#).

After enabling MD5 authentication on ALL your clients, make a small change to add the `notrust` keyword to your NTP Server configuration. This same configuration change is required if you have enabled Stratum 2



operation. The **notrust** keyword forces all associations with the NTP Server to use authentication. Unauthenticated queries to the Server will be ignored.

To add the **notrust** keyword, follow the instructions below. You will need to use a few simple Linux commands and edit keystrokes. If you need help, contact us. There is a brief list of Linux commands on the last page for reference.

Is there an *ntp.conf* file in */boot/etc*?

To see a list of files in */boot/etc*, at the command line type:

```
ls /boot/etc
```

If no, then edit the */etc/ntp.conf* file to add the **notrust** keyword like this:

```
edit /etc/ntp.conf
```

Then add the **notrust** keyword to the restrict statement.

```
restrict default nopeer nomodify noquery notrust
```

After editing the file save it and exit. Then copy to the non-volatile area like this:

```
cp /etc/ntp.conf /boot/etc
```

If yes, then edit the */boot/etc/ntp.conf* file to add the **notrust** keyword like this:

```
edit /boot/etc/ntp.conf
```

Then add the **notrust** keyword to the restrict statement.

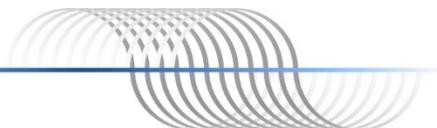
```
restrict default nopeer nomodify noquery notrust
```

After editing the file, save it and exit.

Contact Information:

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

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



Quick Help for Non-Linux Users:

The following commands are available on the command line interface: **ls**, **more**, and **edit**.

ls
ls /etc

List.
This command will display a list of all files in the */etc* directory. Look for the *ntp.conf* file.

more
more /etc/ntp.conf

More.
Use **more** to see what is inside *ntp.conf*.

edit

Edit.
Typing **edit** by itself will display a list of keystrokes you need for using the editor. It will then prompt you for the file name to edit, in this case type: */etc/ntp.conf*.

CTRL-K Q

To quit **edit** without saving.

CTRL-K X

To quit **edit** and save your changes.

cp
cp -p /etc/ntp.conf /boot/etc

Copy.
To copy a file from one location to another. In this case, from */etc* directory to */boot/etc*. The **-p** preserves attributes.

