EndRun TECHNOLOGIES
2270 Northpoint Parkway, Santa Rosa, CA 95407

FIELD SERVICE BULLETIN

FSB# 141222-03

December 22, 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.

Problems:

NTP vulnerability CVE-2014-9293
NTP vulnerability CVE-2014-9294
NTP vulnerability CVE-2014-9295

Vulnerabilities in NTPd before 4.2.8 allow remote attackers to execute code. Details are here:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9293
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9294
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9295

NTP vulnerability CVE-2014-9296

Minor bug discovered in NTPd prior to 4.2.8 related to `crypto`. The NTP developers have not found a way for this bug to affect system integrity. Details for 9296 are here:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9296

Required Action:

Even though the products listed above have a version of NTP prior to 4.2.8, there is an easy way to protect them. No firmware upgrade is required. This mitigation strategy was obtained from the NTP developers at ntp.org: http://support.ntp.org/bin/view/Main/SecurityNotice

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

If no, then edit the */etc/ntp.conf* file and add the **noquery** keyword in the **restrict default...** line like this:

```
restrict default nomodify noquery
```

Then add this line:
```
restrict 127.0.0.1 nomodify
```

Save the file and copy to */boot/etc*.

Then **reboot**.

If yes, then edit the */boot/etc/ntp.conf* file and remove all configuration directives beginning with the **crypto** keyword, if any. Also, make sure the **noquery** keyword is present in the **restrict default...** line. Here is an example:

```
restrict default nomodify noquery
```

And add this line:
```
restrict 127.0.0.1 nomodify
```

Save the file and then **reboot**.

(If you need help with Linux commands see the last page.)

Background Information:

Vulnerability 9296 (**crypto**) is a very minor bug and does not affect system integrity. Vulnerabilities 9293, 9294, and 9295 have to do with NTP remote query tools - **ntpq** and **ntpdc**. There have been known vulnerabilities in remote query for years. The best fix is to restrict the use of **ntpq** and **ntpdc** to local operation only. By restricting access, the vulnerabilities their operation might present are not exposed to outside hosts coming in over the network. If someone is executing either **ntpq** or **ntpdc** while logged into the Sonoma, that's fine. They are already logged in and the idea is that such a person is not a malicious user. Even if they are, they're already in anyway.

2270 Northpoint Parkway, Santa Rosa, CA 95407

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`**, **`cp`**, and **`edit`**.

`ls` **`ls /boot/etc`**	List. This command will display a list of all files in the */boot/etc* directory. Look for the *ntp.conf* file.
`more` **`more /boot/etc/ntp.conf`**	More. Use **`more`** to see what is inside *ntp.conf*.
`edit` **`edit /boot/etc/ntp.conf`**	Edit. Use **`edit`** if you need to make changes to the file.
`ALT-H`	Help Screen. This will show you a list of keystrokes you might need.
`CTRL-K Q`	To quit without saving.
`CTRL-K X`	To quit and save your changes.
`cp` **`cp -p /etc/ntp.conf /boot/etc`**	Copy. To copy a file from one location to another. The **`-p`** preserves attributes.