EndRun
TECHNOLOGIES

2270 Northpoint Parkway, Santa Rosa, CA 95407

FIELD SERVICE BULLETIN

FSB# 140110-01b

January 10, 2014

(Revised 1/24/2014)

Affected Products:

Sonoma Time Servers – all firmware versions.

Part Number:	**Description:**
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.

Problem:

NTP vulnerability CVE-2013-5211

Vulnerability detected in the **`monlist`** feature in **`ntpd`** before version 4.2.7p26. It allows remote attackers to cause a denial of service (traffic amplification). Details are here: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211&cid=1.

Required Action:

This vulnerability has to do with allowing remote execution of the NTP query tools - **`ntpq`** and **`ntpdc`**. Even though Sonoma has a version of NTP prior to 4.2.7p26, it is shipped from the factory with remote execution of these query tools disabled. So, your unit is probably OK. The only way Sonoma might be vulnerable is if you have edited the *ntp.conf* file and saved it in */boot/etc*.

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

If no, then you have nothing to worry about.

If yes, then edit */boot/etc/ntp.conf* and make sure the **`noquery`** keyword is present in the **`restrict default...`** line. Here is an example:

```
restrict default nomodify noquery
```

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

Background Information:

The **`monlist`** vulnerability has 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.

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 /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. 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: */boot/etc/ntp.conf*.
`CTRL-K Q`	To quit without saving.
`CTRL-K X`	To quit and save your changes.