SECURITY BULLETIN

SB# 141222
December 22, 2014

Issue: NTPd Remote Query and Crypto Vulnerabilities

Described 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
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9296

Summary:

NTPd versions prior to 4.2.8 are vulnerable. EndRun products have versions prior to that. However, there will be no immediate firmware upgrade because these vulnerabilities are minor and easily mitigated. Also, products shipped after September 2011 are NOT vulnerable unless you have changed the default configuration in the *ntp.conf* file. If you have an older product, or if you have changed the *ntp.conf* file, then please see the appropriate section below.

As always, we recommend all customers implement Security Best Practices as described in the paper below. It was written for the Sonoma time server but instructions are similar for the older models:
http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

Products:

Sonoma Time Servers are NOT vulnerable unless you have changed the *ntp.conf* file to allow remote query or crypto. See this Field Service Bulletin for more information:
http://www.endruntechnologies.com/pdf/FSB141222-01.pdf

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)