

SECURITY BULLETIN

SB# 160606
June 6, 2016

Issue: June 2016 NTP Security Vulnerability Announcement at ntp.org

The NTP Project released a new version of *ntpd* (4.2.8p8) on June 2, 2016. This release fixed the following vulnerabilities:

CVE-2016-4953: Bad authentication demobilizes ephemeral associations

CVE-2016-4954: Processing spoofed server packets

CVE-2016-4955: Autokey association reset

CVE-2016-4956: Broadcast interleave

CVE-2016-4957: Crypto-NAK crash

Details can be found here:

NTP.org – Network Time Protocol project [June 2016 Security Vulnerability Announcement](#)

Summary: These vulnerabilities are more of a concern for your NTP clients. All clients should be updated to the latest 4.2.8p4 software. Following is the vulnerability impact to EndRun's NTP server products and mitigation steps.

EndRun Technologies Product Impact Statement:

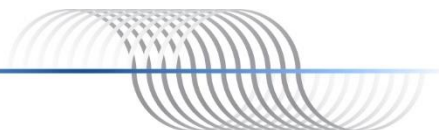
CVE-2016-4953 thru CVE-2016-4956

EndRun's current and legacy NTP server products with the latest firmware and factory-default configuration settings in the *ntp.conf* file are not susceptible. Exceptions are if you have changed the configuration to permit remote control (don't do that), peering, or Stratum 2 operation. EndRun has always recommended against peering as explained here: [About Peering and Stratum 2](#).

CVE-2016-4957

EndRun's current and legacy NTP server products are not susceptible to this vulnerability.

Please see the chart below of the EndRun NTP time server products, respective part numbers, and mitigation steps.



EndRun Technologies NTP Server Products

Current NTP Server Products

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)
3041-xxxx-xxx Tycho II Precision TimeBase
3043-xxxx-xxx Meridian II Precision TimeBase

Mitigation

Do not enable remote control, use peering or Stratum 2 operation.
Update NTP server product software that will be available in August 2016.

Legacy NTP Server Products

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

Mitigation

Do not enable remote control, use peering or Stratum 2 operation.

Note: 'x' is a variable number.

As always, use best practices to keep your time server secure as described here:

[Best Practices to Secure Your Time Server](#)

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
+1-707-573-8633 or 1-877-749-3878 (toll-free in the USA & Canada)
support@endruntechnologies.com

