NETWORK SECURITY BULLETIN
NSB# 180606
June 6, 2018

Issue: February 2018 Security Vulnerability Announcement at ntp.org

The NTP Project released a new version of *ntpd* (v4.2.8p11) on February 27, 2018. This release addressed some informational, low, and medium-level vulnerabilities listed below. Details can be found at the Network Time Protocol project February 2018 Security Vulnerability Announcement.

CVE-2016-1549: Sybil vulnerability: ephemeral association attack

CVE-2018-7182: ctl_getitem(): buffer read overrun leads to undefined behavior and information leak

CVE-2018-7170: Multiple authenticated ephemeral associations

CVE-2018-7184: Interleaved symmetric mode cannot recover from bad state

CVE-2018-7185: Unauthenticated packet can reset authenticated interleaved association

CVE-2018-7183: ntpq:decodearr() can write beyond its buffer limit

EndRun Technologies Product Impact Statement:
All EndRun NTP products with the latest firmware and factory-default configuration settings in the *ntp.conf* file are not susceptible to these vulnerabilities. The only exceptions are if you have changed the configuration to permit remote control (not recommended), peering (not recommended), Stratum 2 operation without authentication, and interleaved mode without authentication. EndRun has always recommended against remote control and peering as explained here: About Peering and Stratum 2. Authentication (MD5 or SHA) is highly recommended and should be used with Stratum 2 and interleaved mode operation.

Since the vulnerability impact to EndRun's products is very limited and easily mitigated, there will be no immediate firmware release. However, you should make sure your product has the most recent firmware. Go here to check: Download Product Firmware.

Regarding your NTP clients, they should be updated to the latest 4.2.8p11 ntpd distribution. It is also highly recommended to configure your clients to use MD5 or SHA authentication as described in the *Use Authentication* section here: Best Practices to Secure Your Time Server. You should also see Field Service Bulletin FSB151026 for details.
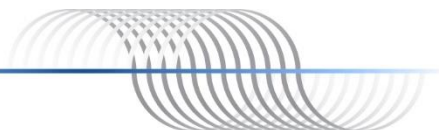
EndRun Technologies Products and Vulnerability

| |
|---|
| **Sonoma Network Time Server**
 Tycho II Precision TimeBase
 Meridian II Precision TimeBase

 Vulnerability: The latest software for these products supports ntpd v4.2.8p9. Refer to the product impact statement above and mitigation steps. The software for these products is periodically updated along with the latest ntpd distribution.

 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 |
| **Tempus LX Network Time Server**
 Unison Network Time Server
 Meridian Precision GPS TimeBase

 Vulnerability: The latest software for these products supports ntpd v4.2.6p3. Refer to the product impact statement above and mitigation steps. The software for these discontinued products is no longer updated therefore the ntpd distribution will remain at v4.2.6p3.

 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 |
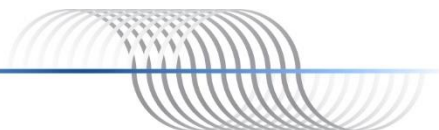
Tycho Frequency Reference
Distribution Chassis (with network port option)

Vulnerability: These products are unaffected as they do not support NTP.

3020-xxxx-xxx   Tycho CDMA Frequency Reference
3021-xxxx-xxx   Tycho GPS Frequency Reference
3204-xxxx-xxx   RTM3204 GPS Timing Module
3300-xxxx-xxx   FDC3300 Frequency Distribution Chassis
3301-xxxx-xxx   PDC3301 Pulse Distribution Chassis
3302-xxxx-xxx   FDC3302 High-Performance Frequency Distribution Chassis
3303-xxxx-xxx   TDC3303 Time Code Distribution Chassis

Note: 'x' is a variable number.

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