NETWORK SECURITY BULLETIN

NSB# 170328

March 28, 2017

Issue: March 2017 NTP Security Vulnerability Announcement at ntp.org

The NTP Project released a new version of *ntpd* (v4.2.8p10) on March 22, 2017. This release addressed some informational, low, and medium-level vulnerabilities listed below. Details can be found at the Network Time Protocol project March 2017 Security Vulnerability Announcement.

CVE-2017-6464 / NTP-01-016 NTP: Denial of Service via Malformed Config.

CVE-2017-6462 / NTP-01-014 NTP: Buffer Overflow in DPTS Clock.

CVE-2017-6463 / NTP-01-012 NTP: Authenticated DoS via Malicious Config Option.

NTP-01-011 NTP: ntpq_stripquotes() returns incorrect Value.

NTP-01-010 NTP: ereallocarray()/eallocarray() underused.

CVE-2017-6455 / NTP-01-009 NTP: Windows: Privileged execution of User Library code.

CVE-2017-6452 / NTP-01-008 NTP: Windows Installer: Stack Buffer Overflow from Command Line.

CVE-2017-6459 / NTP-01-007 NTP: Windows Installer: Data Structure terminated insufficiently.

NTP-01-006 NTP: Copious amounts of Unused Code.

NTP-01-005 NTP: Off-by-one in Oncore GPS Receiver.

CVE-2017-6458 / NTP-01-004 NTP: Potential Overflows in ctl_put() functions.

CVE-2017-6451 / NTP-01-003 Improper use of snprintf() in mx4200_send().

CVE-2017-6460 / NTP-01-002 Buffer Overflow in ntpq when fetching reslist.

NTP-01-001 Makefile does not enforce Security Flags.

CVE-2016-9042 / 0rigin.

These vulnerabilities are more of a concern for your NTP clients. All clients should be updated to the latest 4.2.8p10 ntpd distribution. It is highly recommended to use MD5 or SHA authentication for both your NTP Server and your clients as described in the *Use Authentication* section here: Best Practices to Secure Your Time Server. You can also make a small configuration change to your NTP Server which will further protect your clients. See Field Service Bulletin FSB151026 for details.

EndRun Technologies Product Impact Statement:

All EndRun 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), or Stratum 2 operation 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 operation. Also, avoid unusually long variable names (i.e. 200-512 bytes) in ntpd.conf.

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.

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