EndRun TECHNOLOGIES
"Smarter Timing Solutions"

NETWORK SECURITY BULLETIN

NSB# 151026

October 26, 2015

Issue: October 2015 NTP Security Vulnerability Announcement at ntp.org

The NTP Project released a new version of *ntpd* on Wednesday, Oct. 21. Version number is 4.2.8p4. This release fixed some low- and medium-severity vulnerabilities listed here:

CVE-2015-7871 NAK to the Future: Symmetric association authentication bypass via crypto-NAK (Cisco ASIG)

CVE-2015-7855 *decodenetnum()* will ASSERT botch instead of returning FAIL on some bogus values (IDA)

CVE-2015-7854 Password Length Memory Corruption Vulnerability. (Cisco TALOS)

CVE-2015-7853 Invalid length data provided by a custom refclock driver could cause a buffer overflow. (Cisco TALOS)

CVE-2015-7852 *ntpq atoascii()* Memory Corruption Vulnerability. (Cisco TALOS)

CVE-2015-7851 *saveconfig* Directory Traversal Vulnerability. (OpenVMS) (Cisco TALOS)

CVE-2015-7850 remote config logfile-keyfile. (Cisco TALOS)

CVE-2015-7849 trusted key use-after-free. (Cisco TALOS)

CVE-2015-7848 mode 7 loop counter underrun. (Cisco TALOS)

CVE-2015-7701 Slow memory leak in CRYPTO_ASSOC. (Tenable)

CVE-2015-7703 configuration directives "pidfile" and "driftfile" should only be allowed locally. (RedHat)

CVE-2015-7704, CVE-2015-7705 Clients that receive a KoD should validate the origin timestamp field. (Boston University)

CVE-2015-7691, CVE-2015-7692, CVE-2015-7702 Incomplete autokey data packet length checks. (Tenable)

Details can be found here:

NTP.org – Network Time Protocol project October 2015 Security Vulnerability Announcement

At the link above, the NTP Project states: *The only generally-exploitable bug in the above list is the crypto-NAK bug, which has a CVSS2 score of 6.4.*

These vulnerabilities are more of a concern for your NTP clients. All clients should be updated to the latest 4.2.8p4 software. Use MD5 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 the Field Service Bulletin for details: http://www.endruntechnologies.com/pdf/FSB151026.pdf

EndRun Technologies Product Impact Statement:

All EndRun products with the latest firmware and the 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 (don't do that), peering or Stratum 2 operation.

EndRun has always recommended against peering as explained here: About Peering and Stratum 2.

If you have set up Stratum 2 operation, then you will need to make a small configuration change. You can also help protect your clients by making the same configuration change. See the applicable Field Service Bulletin listed in the next section for detailed instructions.

As always, use best practices to keep your time server secure as described here:
Best Practices to Secure Your Time Server

Since the 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 available. 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: These products are not affected by the listed vulnerabilities unless you have enabled peering or Stratum 2 operation. We have always recommended against peering as explained here: About Peering and Stratum 2. For details on how to make a small configuration change for Stratum 2 then see this Field Service Bulletin: http://www.endruntechnologies.com/pdf/FSB151026.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)
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

If these products have the most recent firmware release, then they are not affected by these vulnerabilities unless you have enabled peering or Stratum 2 operation. We have always recommended against peering as explained here: About Peering and Stratum 2. For details on how to make a small configuration change for Stratum 2 then see this Field Service Bulletin: http://www.endruntechnologies.com/pdf/FSB151026.pdf

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 not affected because they do not use 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