EndRun
TECHNOLOGIES
"Smarter Timing Solutions"

SECURITY BULLETIN
SB# 161205
December 5, 2016

Issue: November 2016 NTP Security Vulnerability Announcement at Ntp.org

The NTP Project released a new version of ntpd (4.2.8p9) on November 21 that addresses the following medium and high (Windows clients only) vulnerabilities:

- Sec 3119 / CVE-2016-9311: Trap crash (affects Windows only)
- Sec 3118 / CVE-2016-9310: Mode 6 unauthenticated trap information disclosure and DDoS vector
- Sec 3114 / CVE-2016-7427: Broadcast Mode Replay Prevention DoS
- Sec 3113 / CVE-2016-7428: Broadcast Mode Poll Interval Enforcement DoS
- Sec 3110 / CVE-2016-9312: Windows: ntpd DoS by oversized UDP packet
- Sec 3102 / CVE-2016-7431: Regression: 010-origin: Zero Origin Timestamp Bypass
- Sec 3082 / CVE-2016-7434: Null pointer dereference in _IO_str_init_static_internal()
- Sec 3072 / CVE-2016-7429: Interface selection attack
- Sec 3071 / CVE-2016-7426: Client rate limiting and server responses
- Sec 3067 / CVE-2016-7433: Reboot sync calculation problem

Vulnerability details are listed in VU#633847.

Summary
EndRun's Network Time Servers (Sonoma, Tempus, Unison) and Precision TimeBase (Meridian II, Tycho II, Meridian) operating with the factory default configuration (i.e. no remote access to ntpdc and ntpq, no peering, no traps, and no rate limiting) are not affected by these vulnerabilities.

A future software release for EndRun's current NTP products will update the ntpd version to 4.2.8p9.   It is recommended that ntpd clients (especially Windows clients) update to the latest 4.2.8.p9 distribution now.

EndRun NTP Server Products Vulnerability Impact and Mitigation

Current NTP Server Products with ntpd 4.2.8p8

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
EndRun's current 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 to ntpdc/ntpq, peering, traps or rate limiting. EndRun has always recommended against remote control and peering as explained here: About Peering and Stratum 2.

Update Linux Subsystem software that will include ntpd 4.2.8p9 or later when available.

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

EndRun's 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 to ntpdc/ntpq, peering, traps or rate limiting. EndRun has always recommended against remote control and peering as explained here: About Peering and Stratum 2.

No updates to the Linux Subsystem software are planned as the products are discontinued.

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