

NETWORK SECURITY BULLETIN

NSB# 150414

April 14, 2015

Issue: NTP Client/Peering Vulnerabilities

A vulnerability in the NTP Project ntpd reference has been identified that could impact operation in peering mode with symmetric key cryptography. All NTP4 releases starting with ntp-4.2.5p99 up to but not including ntp-4.2.8p2 are vulnerable to this issue.

Details on this vulnerability can be found on the following websites:

NTP.org - Network Time Protocol project: [April 2015 Security Notice](#)

NIST National Vulnerability Database: [Vulnerability Summary for CVE-2015-1799](#)

[Vulnerability Summary for CVE-2015-1798](#)

Software Engineering Institute: [Vulnerability Note VU#374268](#)

EndRun Technologies Product Impact Statement:

EndRun products that support NTP not configured to use peering are not vulnerable to this issue.

The vulnerability has to do with an NTP Client authenticating a remote server or peer. EndRun has always recommended against peering per this application note [About Peering and Stratum 2](#). As always, use best practices to keep your time server secure as described in this application note: [Best Practices to Secure Your Time Server](#).

EndRun Technologies Products and Vulnerability:

Sonoma Network Time Servers:

Vulnerability: These products are not affected unless you are peering multiple servers.

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)



Tempus & Unison Network Time Servers Meridian Precision GPS TimeBase

Vulnerability: These products are not affected unless you are peering multiple servers.

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

Praecis and Tempus Network Time Servers

Vulnerability: These products are not affected, even if you do use peering, because the NTP version is not affected.

3003-xxxx-xxx	Praecis Cntp Network Time Server
3005-xxxx-xxx	Praecis Gntp Network Time Server
3007-xxxx-xxx	Praecis Cntp Network Time Server
3009-xxxx-xxx	Praecis Gntp Network Time Server
3012-xxxx-xxx	Tempus Gntp Network Time Server
3013-xxxx-xxx	Tempus Cntp Network Time Server

Tycho GPS/CDMA Frequency Reference Time Code/Frequency Distribution Chassis

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

**EndRun
TECHNOLOGIES**

"Smarter Timing Solutions"

Santa Rosa, CA, USA
1-877-749-3878 or 707-573-8633
sales@endruntechnologies.com
www.endruntechnologies.com

