EndRun
TECHNOLOGIES
"Smarter Timing Solutions"

SECURITY BULLETIN
SB# 150130
January 30, 2015

Issue: Ghost Vulnerability
Described here: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235

Summary:
EndRun products do use a vulnerable version of the glibc library. However, the remotely accessible protocols running on the EndRun products and required for operation of these products have been determined not to be exploitable, for various reasons. These include openssh, apache and ntpd.

The Ghost vulnerability is very difficult to exploit, even if a protocol happens to be using the gethostbyname() glibc library routines. Most protocols used in EndRun products are not using the gethostbyname() routines because these routines do not support IPv6. Other protocols may use these routines but do checks prior to calling them so that invalid data will not be passed.

Due to the exploitation difficulty and the very small attack surface exposed by the Ghost vulnerability in our products, we will not be introducing a file system upgrade immediately. In the meantime, we strongly recommend disabling all protocols not necessary for performing the products' specific function of providing time to networked computers, and restricting access via a firewall.

As always, we recommend all customers implement Security Best Practices as described in the paper below. It was written for the Sonoma time server but instructions are similar for the Tempus and Unison:
http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

Products:

Sonoma Time Servers are affected. A Linux file system upgrade will be available in 2015. In the meantime, restrict access via a firewall and implement Security Best Practices as described here:
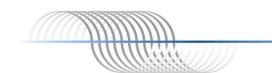http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

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)

The products listed below are affected. A Linux file system upgrade is not available. Disable all unnecessary protocols and restrict access. See your User Manual, Appendix A – Security for instructions. User Manuals are listed here:
http://www.endruntechnologies.com/documentation.htm#disc

3012-xxxx-xxx   Tempus Gntp Network Time Server
3013-xxxx-xxx   Tempus Cntp Network Time Server
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

The products listed below are affected. A Linux file system upgrade is not available. Disable all unnecessary protocols and restrict access. See your User Manual, Appendix D – Security for instructions. User Manuals are listed here:
http://www.endruntechnologies.com/documentation.htm#disc

3204-xxxx-xxx	RTM3204 GPS Timing Module
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

Lantronix Network Port – waiting for information.

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

The optional network port on the Distribution Chassis is a Lantronix XPORT-AR. We are waiting for information to be published at lantronix.com regarding the Ghost Vulnerability. In the meantime, restrict access via a firewall.

Note: 'x' is a variable number.

For more information on Leap Seconds go to this webpage: www.endruntechnologies.com/leap.htm

If you would like to be put on the Customer Support email list to receive a Leap Second Bulletin the next time there is a leap second insertion pending, then email the support address above.

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