SECURITY BULLETIN

SB# 160321

March 21, 2016

Issue: GNU glibc Vulnerability to Arbitrary Code Execution and Denial of Service Via Crafted DNS Reponses

Described here: **CVE-2015-7547**

Summary:
EndRun's Sonoma Network Time Servers, Meridian II/ Tycho II Precision TimeBase, and Distribution Chassis products are not vulnerable.

EndRun's legacy products are vulnerable.

Products: Not Vulnerable to CVE-2015-7547

Part Number	Description
3043-xxxx-xxx	Meridian II Precision TimeBase
3041-xxxx-xxx	Tycho II Precision TimeBase
3029-xxxx-xxx	Sonoma N12 Network Time Server (GPS)
3028-xxxx-xxx	Sonoma N12 Network Time Server (CDMA)
3027-xxxx-xxx	Sonoma D12 Network Time Server (GPS)
3026-xxxx-xxx	Sonoma D12 Network Time Server (CDMA)
3303-xxxx-xxx	TDC3303 Time Code Distribution Chassis
3302-xxxx-xxx	FDC3302 High-Performance Frequency Distribution Chassis
3301-xxxx-xxx	PDC3301 Pulse Distribution Chassis
3300-xxxx-xxx	FDC3300 Frequency Distribution Chassis

Products: Vulnerable to CVE-2015-7547

Part Number	Description
3025-xxxx-xxx	Meridian CDMA Frequency Reference
3021-xxxx-xxx	Tycho GPS Frequency Reference
3020-xxxx-xxx	Tycho CDMA Frequency Reference
3019-xxxx-xxx	Meridian Precision GPS TimeBase
3018-xxxx-xxx	Tempus LX CDMA Network Time Server (Japan)
3017-xxxx-xxx	Unison GPS Network Time Server
3016-xxxx-xxx	Unison CDMA Network Time Server
3015-xxxx-xxx	Tempus LX GPS Network Time Server
3014-xxxx-xxx	Tempus LX CDMA Network Time Server
3009-xxxx-xxx	Praecis Gntp Network Time Server
3012-xxxx-xxx	Tempus Gntp Network Time Server
3204-xxxx-xxx	RTM3204 GPS Timing Module

Mitigation

Since the EndRun products vulnerable to this issue are legacy, a software update is not currently planned. In order to exploit this vulnerability, an attacker would have to control the domain and respective DNS server to craft a response. Although this limits the risk, the following steps could be used to further reduce risk:

1. Do not specify a DNS server
   Without a DNS server configured, no external DNS queries will be made precluding receipt of crafted DNS responses. The EndRun web server, however, will not run without DNS so it should be disabled as well.

2. Trusted internal DNS server
   Specifying a local, trusted DNS resolver can mitigate risk to this vulnerability if the resolver sanitizes incoming responses.

Contact Information:

Feel free to contact us if you have any questions or need help:

EndRun Technologies
2270 Northpoint Parkway, Santa Rosa, CA 95407 U.S.A.
+1-707-573-8633 or 1-877-749-3878 (toll-free)
support@endruntechnologies.com