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