PSIB 20170124A Meinberg WebUI Security Advisory Service

Date: May 1, 2019

Summary:

Meinberg Time Servers, specifically LTOS6 based firmware products, have been identified as having security vulnerabilities, which may allow escalation to super user (admin) privileges. Affected systems are all LANTIME, SyncFire, and LCES firmware versions before 6.20.005. The Net Time Protocol (NTP) project of the Network Time Foundation recently released ntp-4.2.8p8, patching a number of low severity vulnerabilities and one high severity vulnerability. According to cert.org, due to the vulnerabilities unauthenticated, remote attackers may be able to spoof or send specially crafted packets to create denial of service conditions. Meinberg therefore strongly recommends updating your LANTIME devices as soon as possible by installing LTOS 6.20.005 or later.

Affected Products:

- Meinberg time servers with V5 or V6 firmware

Recommendations:

Meinberg has released a new firmware version 6.20.005 to address these vulnerabilities, which can be downloaded at the following location:
https://www.meinbergglobal.com/english/sw/firmware.htm

For V5 and V6 versions of firmware, it is strongly encouraged to update to 6.20.005 or later as soon as possible. Please contact Meinberg support for additional assistance.

Attachments PSIB 20170124A.pdf

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0023180

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.