DDoS Attacks on NTP Servers affecting some GNSS receivers

800 Freddy Blume November 23, 2015 Javad, Trimble NetR5, Trimble NetR8, Trimble NetR9 3783

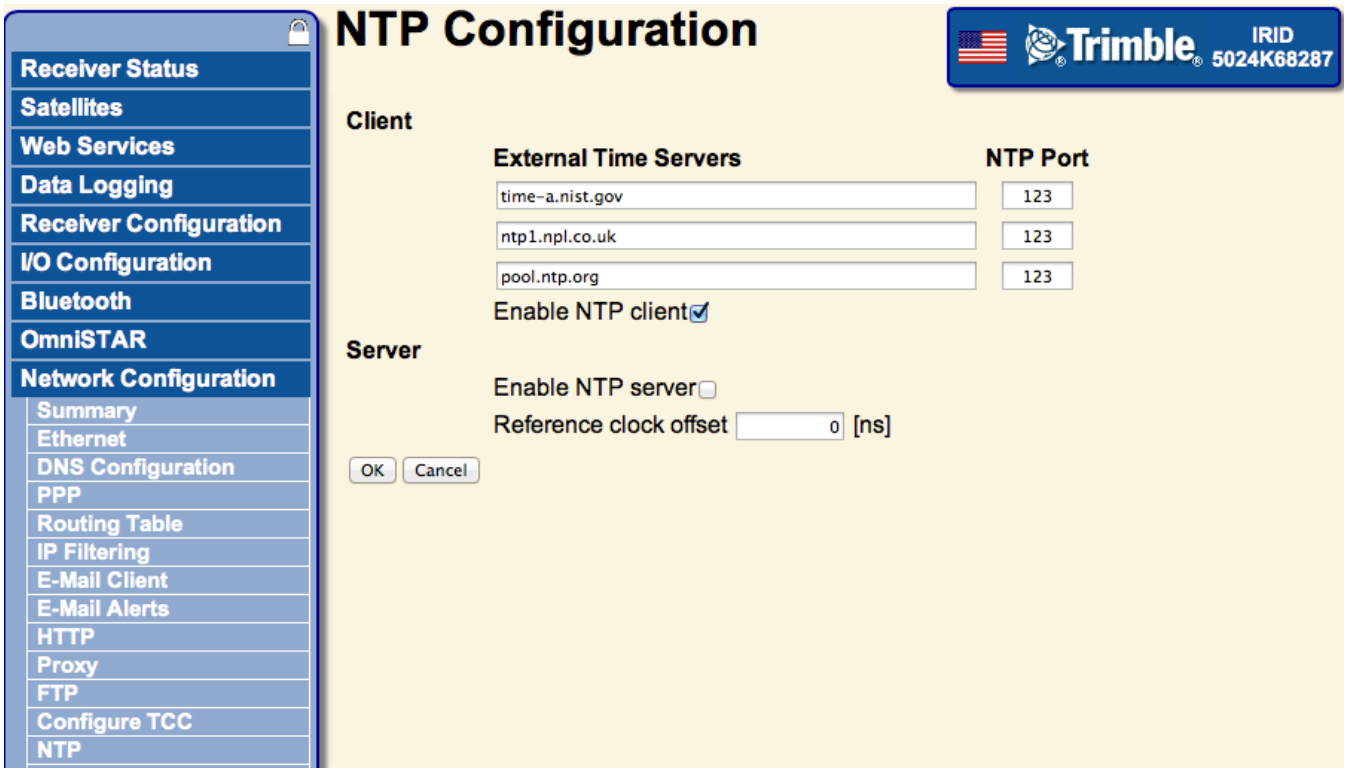
There have recently been widespread attacks by internet gamers on Network Time (NTP) servers - many computers, servers, and devices run these, and some GNSS receivers have proven to be vulnerable.

See this article for a good description of the issue:
NTP Amplification Flaw To Blame For Gaming DDoS Attacks | Threatpost

Our immediate recommendation is that any new-generation JAVAD or Trimble NetR5, NetR8, or NetR9 GNSS receiver (with firmware versions 4.81 or earlier) that has a direct connection to the internet - i.e. a public IP address with no firewall router, cellular modem or VSAT/BGAN in its communication path - should have its NTP server disabled and/or IP Filtering enabled as soon as possible.

NTP servers are left enabled by default on these devices although only a small minority of users require this functionality.

The server can be disabled in the "Network Configuration -> NTP" tab of a Trimble NetR5, NetR8, or NetR9 on the web interface. The recommended configuration will be:



Please see the following Trimble Document for general recommendations regarding the internet security of their devices:
Trimble NetRx Series Receivers: Security Features, Guidelines, and Recommendations

14 February, 2014: Trimble released firmware version 4.85 for NetR5, NetR8, and NetR9 that eliminates the NTP vulnerablity along with many other features and fixes. 4.85 is currently under formal evaluation by the UNAVCO Development and Testing group and will be posted on appropriate KnowledgeBase pages. In the meantime qulafied users can download the firmware and find release notes at Trimble's support page.

Any current-generation JAVAD receivers with similar data communications should have their NTP servers moved to an alternate port; (it is not possible to disable the server) using the follwing GREIS commands, the second of which will restart the receiver:

set,/par/net/ntp/port,1234
set,/par/reset,yes

Trimble NetRS and other brands of GNSS receivers do NOT appear to be vulnerable to these attacks, but we still recommend that all internet security on any device be reviewed for possible vulnerability to this and other threats.

Super-users and system administrators may run a diagnostic command to determine if any given device is vulnerable or under attack to the current NTP (replacing the X's with the IP address or URL of your device)

sudo nmap -sU -pU:123 -Pn -n --script=ntp-monlist XXX.XXX.XXX.XXX

An immediate response that shows a large number of connected servers indicates that the device is currently under attack, while a delayed response indicates that the device is not vulnerable.

If you are operating any other devices with direct internet exposure you should contact your local IT Staff to determine whether a vulnerability needs to be addressed.

Please subscribe to this article in the upper right corner of this page to be notified of updates.

Online URL:
https://kb.unavco.org/article/ddos-attacks-on-ntp-servers-affecting-some-gnss-receivers-800.html