26 October 2012

Trimble NetRx Series Receivers: Security Features, Guidelines, and Recommendations

The Trimble® NetRx series of reference receivers (NetRS®, NetR3, NetR5™, NetR8™, and NetR9™) have various security features built into the receiver firmware. As recent trends within the industry point to ever-increasing cyber-attacks, Trimble strongly recommends using the latest released build of firmware for these receiver platforms as well as reviewing the security implementations set in the receiver firmware.

While Trimble NetRx series receivers contain several security features hard-coded in the firmware, you must configure others. This document outlines the security features of the NetRx series receivers and provides general security guidelines and recommendations on improving a receiver's security.

Firmware

Trimble regularly releases updated firmware containing various enhancements and new functionalities. Trimble strongly recommends that receivers are upgraded to the current firmware to take advantage of new features—new releases often contain security updates to deal with the evolving industry and new security threats. To download the firmware, go to www.trimble.com and then go to the required product support page.

Restrict visibility

When installing a NetRx receiver on a network, restrict the receiver Web UI access to a private LAN if possible. By not providing receiver access to the general Internet, you will greatly reduce the opportunity for entities to access the receiver with malicious intent.

Regardless whether the receiver is on a private or public network, IP filtering enables you to limit access to a specific device or group of devices defined by the operator. Trimble strongly recommends using IP Filtering as it is highly effective at limiting access to the receiver controls to only those devices specified by the operator.

If the receiver must be located on the open Internet, you could also install the receiver behind a firewall and only grant access to the receiver ports required by the application.

This document is for informational purposes only and is not a legally binding agreement or offer.
Trimble makes no warranties and assumes no obligations or liabilities hereunder.

Restrict access

Trimble NetRx series receivers offer several layers of user access. By enabling security on the receiver Web UI, the operator can require login authentication to access the receiver and provide various levels of user access, depending upon the receiver model in use.

When configuring HTTP or HTTPS, using non-default ports (ports 80 and 443) can reduce the likelihood of users accidently discovering the port.

Limit data flow

When streaming data to only one client from an individual port, it is recommended that you set the output of the port to Client mode so that the receiver sends the data to the remote client (as opposed to leaving the port open so that anyone can attempt to access the port).

Additionally, some models of the Trimble NetRx series receivers support NTRIP Client, NTRIP Caster, and NTRIP Server capabilities that require authentication on streaming data.

Alerting

For Trimble NetRx series receivers that support email alerts, it is highly recommended to enable and use these features to notify users of changes to the receiver controls, reboots, incorrect logins, and so on. This can quickly alert the operator to suspicious activity in real-time.