

Rugged Operating system on Linux (ROX) Release Notes v1.13.4

April 24th, 2009
Copyright © 2009 RuggedCom Inc.

Summary

Overview.....	2
User Guides.....	2
Changes in v1.13.4 (1790).....	3
net-snmp 5.4.1 for ROX 1.13.4 (Ma 1789).....	3
Deleted SNMPv3 User is still shown on SNMP usmuser table (Ma 1778).....	3
SNMPv3 access control settings cause snmpd to stop (Ma 1705).....	3
ROX Serial DNP fails (Ma 1619).....	3
SNMPv3 - ROX fails to generate SNMPv3 Traps (Ma 1655).....	3
GRE not working after wanrouter restarted (Ma 1683).....	3
Adapt netlink patch to recent net-snmp (Ma 1500).....	3
SNMPD has memory leak and crash sometime (Ma 1452).....	4
Trace function for DDS in Frame Relay mode broken (Ma 1638).....	4
Invalid DNS server makes Webmin slow to serve pages (Mi 1511).....	4
Webmin and time zone changes (Mi 1574).....	4
Webmin accept illegal character (Mi 1621).....	4
Unable to clear the Frame Relay interface statistics (Mi 1623).....	4
SerServer stop running when using TCPModbus (Mi 1649).....	4
Quagga doesn't restart after NTP server restarted (Mi 1680).....	4
Webmin allows the taken 24th time slot to be configured (Mi 1681).....	4
Traffic Control rules on the modem PPP link is broken (Mi 1682).....	4
Dummy interface is accepting invalid IP address (Mi 1742).....	5
FrameRelay configuration accept invalid DLCI number (Mi 1762).....	5
Radius Server Adjustements (Mi 1700).....	5
Cannot set static routes w. gw. field set over /32 PPP links(Mi 1820).....	5
GMT/UTC time options (E 1607).....	5
Cellular Modem Support (E 1118).....	5
Improve GOOSE tunnels performance (E 1771).....	5
Security Updates.....	6
SNMPv3 Authentication Bypass Vulnerability (CVE-2008-0960).....	6
Integer overflow in net-snmp (CVE-2008-4309).....	6
Buffer overflow in the __snprint_value function (CVE-2008-2292).....	6
SNMPv3 HMAC verification vulnerability (CVE-2008-0960).....	6
Upgrade Instructions.....	7
Type of Changes.....	8

Contacting RuggedCom.....9

Overview

ROX™ v1.13.4 Build on ROX 1.13.3 to add an updated SNMP agent that addresses CPU and memory usage concerns. It also includes an updated net-snmp linkUp/Down trap mechanism. Also, several bug fixes were back-ported from the current 1.14.0 development.

IMPORTANT NOTE: An initial upgrade to version either 1.12.4, 1.12.5 or 1.12.6 is needed *before doing an upgrade to 1.13.0, 1.13.1, 1.13.2, 1.13.3 or 1.13.4*, if the current RuggedRouter to be upgraded has a disk usage of 60% or more (as shown on Webmin's main page). Failure to do so may result in a non-functional router.

IMPORTANT NOTE: Do not use the Automatic Upgrade when the ROX version is not of the 1.13.x series.

User Guides

All user guides are available from the RuggedCom Web site at www.RuggedCom.com. Please refer to the ROX 1.13.3 user guide.

Changes in v1.13.4 (1790)

net-snmp 5.4.1 for ROX 1.13.4 (Ma 1789)

Products: RX1000, RX1100

This update brings a new net-snmp version to the ROX 1.13.4 environment. Previous net-snmp version was 5.2.3-7. The updated net-snmp is of version 5.4.1 and fixes CPU over consumption as well as memory leaks. It also features a new link Up/Down trap mechanism.

Deleted SNMPv3 User is still shown on SNMP usmuser table (Ma 1778)

Products: RX1000, RX1100

This update addresses a problem found in the deletion of V3 users. The created V3 users would not be properly deleted.

SNMPv3 access control settings cause snmpd to stop (Ma 1705)

Products: RX1000, RX1100

This update concerns the ability of viewing newly-configured V3 users. In order to view these newly-created users the snmp daemon must be running. A note to that effect reminds the user in the Acces Control page.

ROX Serial DNP fails (Ma 1619)

Products: RX1000, RX1100

Removed extra debugging messages which introduced delays in processing and caused restarting of the serial server.

SNMPv3 - ROX fails to generate SNMPv3 Traps (Ma 1655)

Products: RX1000, RX1100

This update fixes a problem in sending V3 link Up/Down traps.

GRE not working after wanrouter restarted (Ma 1683)

Products: RX1000, RX1100

GRE tunnel up/down state is now linked with the WAN interface so that the tunnel is automatically re-enabled according to the interface state.

Adapt netlink patch to recent net-snmp (Ma 1500)

Products: RX1000, RX1100

This update consists of an update mechanism to send link Up/Down traps.

SNMPD has memory leak and crash sometime (Ma 1452)

Products: RX1000, RX1100

This update fixes memory leaks as well as excessive CPU consumption.

Trace function for DDS in Frame Relay mode broken (Ma 1638)

Products: RX1000, RX1100

When doing a trace using DDS 56K interface cards the following was shown: 'Unknown Configured Wanpipe Protocol 0x88' instead of the trace data. The WAN monitor component was updated.

Invalid DNS server makes Webmin slow to serve pages (Mi 1511)

Products: RX1000, RX1100

A miniserv configuration option adjustment made Webmin keep the same response time in any cases.

Webmin and time zone changes (Mi 1574)

Products: RX1000, RX1100

Previously, Webmin did not react to time zone changes.

Webmin accept illegal character (Mi 1621)

Products: RX1000, RX1100

Minor improvement concerning the Webmin data entry field for IPsec configuration.

Unable to clear the Frame Relay interface statistics (Mi 1623)

Products: RX1000, RX1100

Frame Relay interface statistics could not be cleared.

SerServer stop running when using TCPModbus (Mi 1649)

Products: RX1000, RX1100

When configuring TCPModbus for several serial ports, the serial server process would not restart once configured in the 'Bootup and Shutdown' menu. An adjustment in the serial server now handles this situation.

Quagga doesn't restart after NTP server restarted (Mi 1680)

Products: RX1000, RX1100

An update of the script used to start/restart Quagga fixed the use of the ntp_corr variable.

Webmin allows the taken 24th time slot to be configured (Mi 1681)

Products: RX1000, RX1100

The 24th time slot had been taken by the 2nd channel of the T1-1 port, but 1st channel still can use this taken slot. The Webmin configuration was changed to prevent this.

Traffic Control rules on the modem PPP link is broken (Mi 1682)

Products: RX1000, RX1100

TC rules configured under the Shorewall do not take place when the PPP0 interface is down and brought back up later. However, the rules are working fine if the Firewall Configuration is reapplied after the PPP0 interface is brought back up. Resolving this problem consisted of synchronizing

Shorewall with the ppp interface.

Dummy interface is accepting invalid IP address (Mi 1742)

Products: RX1000, RX1100

Webmin was updated in order to better validate user input for the dummy interface.

FrameRelay configuration accept invalid DLCI number (Mi 1762)

Products: RX1000, RX1100

This concerns a problem in filtering out invalid user entry for the DLCI values.

Radius Server Adjustments (Mi 1700)

Products: RX1000, RX1100

In some occasions a Radius server would expect additional fields to be communicated such as the Vendor-Specific field. This adjustment enables better compatibility with differently-configured Radius servers. Another adjustment consisted of testing a somewhat slower response and suggesting a timeout of 10 seconds in those circumstances.

Cannot set static routes w. gw. field set over /32 PPP links(Mi 1820)

Products: RX1000, RX1100

Verification of a valid address and netmask were added for /32 static PPP links.

GMT/UTC time options (E 1607)

Products: RX1000, RX1100

This is an enhancement to the current Webmin System Time page to provide GMT and DST settings. This is useful for customers who like to maintain a constant time base, not subject to daylight savings time (DST) in a distributed network.

Cellular Modem Support (E 1118)

Products: RX1000, RX1100

This enhancement improves the verbosity of cellular modem related events in order to better assess the state of a link.

Improve GOOSE tunnels performance (E 1771)

Products: RX1000, RX1100

This enhancement improves performance of the GOOSE tunneling by approx. 10 times.

Security Updates

SNMPv3 Authentication Bypass Vulnerability (CVE-2008-0960)

Component: net-snmp

Overview: A vulnerability in the way implementations of SNMPv3 handle specially crafted packets may allow authentication bypass.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960>

Integer overflow in net-snmp (CVE-2008-4309)

Component: net-snmp

Overview: Integer overflow in the netsnmp_create_subtree_cache function in agent/snmp_agent.c in net-snmp 5.4 before 5.4.2.1, 5.3 before 5.3.2.3, and 5.2 before 5.2.5.1 allows remote attackers to cause a denial of service (crash) via a crafted SNMP GETBULK request, which triggers a heap-based buffer overflow, related to the number of responses or repeats.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4309>

Buffer overflow in the __snprint_value function (CVE-2008-2292)

Component: net-snmp

Overview: Buffer overflow in the __snprint_value function in snmp_get in Net-SNMP 5.1.4, 5.2.4, and 5.4.1, as used in SNMP.xs for Perl, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large OCTETSTRING in an attribute value pair (AVP).

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2292>

SNMPv3 HMAC verification vulnerability (CVE-2008-0960)

Component: net-snmp

Overview: SNMPv3 HMAC verification in (1) Net-SNMP 5.2.x before 5.2.4.1, 5.3.x before 5.3.2.1, and 5.4.x before 5.4.1.1.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960>

Upgrade Instructions

Before upgrading we recommend:

- Reviewing all the changes to ensure an upgrade is merited.
- Upgrading a test unit to ensure you understand the upgrade process.
- Planning for a temporary network outage.

The upgrade procedure works by using a set of upgrade files accessible from a web server. These files are distributed in the form of a .zip archive and should be unpacked in a location on a web server that's accessible from the router. Using Webmin Upgrade -> System on a router, the configuration is made using 'Change Repository Server' to point to that location on the web server. Once done, a test run of the upgrade can be made by setting the 'Only show which packages would be upgraded' option to Yes and doing an 'Upgrade Now'. When everything is found satisfactory, setting the same option to No and doing an 'Upgrade Now' will actually launch the upgrade process. Depending on the nature of the upgrade, you might be asked to confirm if a reboot of the unit is deemed necessary. It is important that there are no power supply interruption during the time it takes for an upgrade to complete. The following illustration highlights the various options used in the process of upgrading a RuggedRouter.

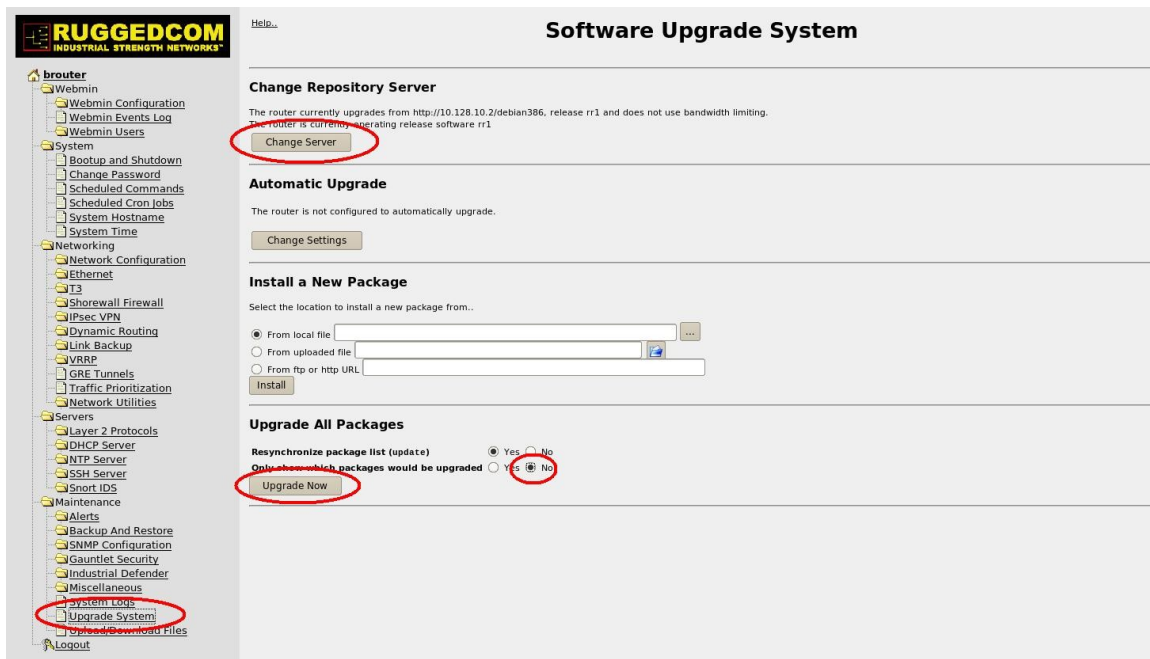


Illustration 1: ROX Upgrade Process using Webmin

Type of Changes

Each change to the firmware is categorized according to the table below to provide a guide as to whether the change justifies upgrading. As well, each change lists an internal RuggedCom change number.

Change Type	Description
Critical (C)	Critical changes fix problems that prevent the basic operation of the device and have no workaround. Any critical changes merit a device upgrade under all circumstances.
Major (Ma)	Major changes fix problems that prevent the basic operation of the device but do have a workaround. Any major changes merit a device upgrade if the workaround is not acceptable.
New Feature (NF)	New features add significant new capability to the device. Such changes may change the basic operation of the device, the user interface, and how the device is configured. New features only merit a device upgrade if the feature is required.
Enhancement (E)	Enhancements improve existing device capability and do not significantly change the basic operation of the device, the user interface, or how the device is configured. Enhancements only merit a device upgrade if the feature is required.
Minor (Mi)	Minor changes fix non-vital problems that may or may not have a workaround. Minor changes do not necessarily merit a device upgrade unless the specific problem applies.
Cosmetic (Co)	Cosmetic changes have negligible impact on device operation and include such updates as spelling mistakes, user interface adjustments, and help text improvements. Cosmetic changes rarely merit a device upgrade.

Contacting RuggedCom

Corporate Headquarters

RuggedCom Inc.
30 Whitmore Road
Woodbridge, Ontario
Canada, L4L 7Z4

Toll-free: 1(888) 264-0006
Tel: (905) 856-5288
Fax: (905) 856-1995

US Corporate Headquarters

RuggedCom
1930 Harrison St. Suite 307
Hollywood, Florida
USA 33020
Tel.: (954) 922-7975

Technical Support

Toll Free: 1 866 922-7975

Web: www.RuggedCom.com
Email: support@RuggedCom.com