Release Note NRSW 4.8.0.100

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.8.0.100. It informs on new functionality, corrections and known issues of this software version of NetModule's router series.

Keywords:

NetModule, Software Development, NRSW, Release Note

Document Control:

Document:	Version	1.0
	File	NRSW-RN-4.8.0.100
	Status	Final

Creation:	**Role**	**Name**
	Author	Felix Kopf
	Review	Stefan Leuenberger

Approval	**Role**	**Name**
	Director Product Development	Benjamin Amsler

1 Release Information

NetModule Router Software:

Version:	**4.8.0.100**
Date:	**Jun 14, 2023**

Supported Hardware:

NetModule Router	Hardware Version
NB800	V2.0 - V2.2, V3.2 (Rev. B02)
NG800	V3.0 - V3.1
NB1601	V1.0 - V1.6
NB1800	V2.4 - V2.6
NB1810	V2.4 - V2.6
NB2800	V1.0 - V1.4
NB2810	V1.2
NB3701	V1.0 - V1.10
NB3800	V1.0 - V1.10

Unsupported Hardware:

NetModule Router
NB1300 Series
NB1600 Series
NB2200 Series
NB2300 Series
NB2500 Series
NB2600 Series
NB2700 Series
NB3700 Series
NB3711

NetModule Insights
Subscribe to our mailing and get the latest news
about software releases and much more

2 New Features

Case-#	Description
65258	**IPSec** A configurable dead peer detection for IKEv2 based tunnels has been added.
69107	**Mobile provider database updated** The APN "home.vodafone.de" has been added to the mobile provider database and can be selected in the web interface now.
73519	**RSTP** RSTP status data is now visible via cli, sdk, and the web interface.
75659	**Virtualization** MAC addresses of ethernet interfaces for lxc containers can now be configured manually.
75795	**Access Controller (AC) WLAN** For the configuration and management of AP3400, access points. The AC is able to generate AP3400 configurations, push the configuration, and read the current status information of AP3400 devices. The AC can manage up to 15 AP3400 devices. It will be distinguished between different device state
78238	**Firewall features** Unencrypted outgoing traffic is now actively rejected during IPSec tunnel downtimes.
78942	**WLAN firmware updates** Router NG800, NB800, and NB1601 (TI WL18xx-based WLAN module) will use the new WLAN module firmware "8.9.0.0.90"
78943	**3rd party open source packages updated** hostapd/wpa-supplicant updated to latest 2.10 version iw updated to version 5.19 mac80211 updated to version v5.15.58 ath10k-ct updated to version 22
80049	**DHCP improvements** DHCP can now assign static hosts identified by their hostname, previously only MAC-Address and Client ID (labeled as hostname) where supported.
81284	**Web interface** The report of the status of L2TP tunnels has been added the "summary" dashboard.
81984	**SDK improvements** The SDK-function nb_transfer_post can now be used to send raw data such as JSON-formatted data to a remote server, additionally to sending files.
82153	**NTP Server** The allowed hosts of the NTP Server will now be updated automatically when the IP configuration is changed.
82222 82414	**ITxPT** The smc routing daemon can now be configured to be available on multiple network interfaces. mDNS requests can now be forwarded to multiple interfaces.
82230	**NAPT rules** The maximum number of incoming NAPT rules has been increased to 100.
82288	**CAN utitlities extended** The existing can-utility suite has been extended by new commandline tools: canbusload, can-calc-bit-timing, canlogserver, canfdtest, canplayer, cangw and cangen.
82397	**iperf3** The command line tool iperf3 has been added to the routers file system and can be used from console.

Case-#	Description
82525	**Support for new WWAN modules** The NRSW now supports u-blox LTE module LARA-L6. Router Hardware dependency has to be considered.
82672 **82673**	**GNSS Modules** Support for new GNSS module u-blox NEO-M9 was added. Support for new GNSS module u-blox MAX-M10 was added.

3 Security Fixes

The following security relevant issues have been fixed.

Case-#	Description
79309	**Web interface improvements** Autocomplete attributes were added to password field to inform the browser, whether passwords should be stored.
81746	**WLAN** CVE-2022-42719: A use-after-free in the mac80211 stack when parsing a multi-BSSID element could be used by attackers to crash the kernel and potentially execute code.
83009	**Security fix for Let's Encrypt** Let's Encrypt had a remote code execution issue in the acme.sh script. This is fixed.

4 Fixes

The following issues and problems have been fixed.

Case-#	Description
73892 **77702** **81124** **81483**	**Web interface improvements** On certain pages, the footer elements where displayed incorrectly, this issue was fixed. The scan for available wireless networks now provides more detailed information. The system log display is no longer jumping to the first line each time a new message arrives. The upload of QR code images for eSIM profiles has been fixed.
75482 **82355**	**Network fixes** Switching link prioritization was deficient since 4.4.0.104. This is fixed A mismatch of the MTU size configured for LE910C4-EU modems caused fragmentation issues, this has been fixed.
77188	**DHCP improvements** DHCP can now be configured for BR interfaces.
78449 **82156** **82922**	**Web interface** The error message that was shown, when a login attempt was made with a wrong CSRF token was fixed to be more helpful. When configuring a new IP address for the interface that is currently used for reaching the web interface, the browser will be redirected to the newly configured address. The web interface for ITxPT now highlights the correct sub menu in the navigation panel on the left side.
78719 **81711** **82112**	**ITxPT** ITxPT inventory status now shows 1 instead of 0 on system error. The multicast TTL can now be configured in the web interface. The ITxPT MQTT service was not announced in mDNS, because of a missing symlink.
78724	**ssh authentication** In previous releases, the user "admin" was not able to authenticate ssh sessions by using an uploaded public key. This issue has been fixed.
79734	**WWAN connections** The network registration process of modems from the Ublox TOBY-L2 series has been improved.
80543	**LLDP** The LLDP daemon (lldpd) was only started on every second attempt when changing protocols for a currently active lldpd. This issue has been fixed.
80994	**User Interface** In previous versions, the underscore symbol was rejected in the username and password fields for the automatic configuration update mechanism. This issue was fixed.
81438	**Improved handling of virtual wlan interfaces** Virtual interfaces can now be enabled and disabled, keeping their configuration.
81573	**GUI** While changing the LAN IP address range the DHCP server range notification pop-up was missing.
81669	**Configuration upload** The upload of larger configurations could result in the router running in a timeout and as a consequence ending up in an error state. This issue has been fixed.
81684	**Watchdog fixes** Watchdog had a memory leak since 4.6.0.100. This is fixed.
82083	**Modem fixes** TOBY-L2 modems were not reset properly, this issue has been fixed.

Case-#	Description
82255	**Serial Console** A misconfiguration of the serial console caused output on the serial port when it was disabled, this has been fixed.
82376 **82408**	**IPsec improvements** Shared networks were not routed correctly when trying to access them directly from the tunnel end-point and thus were not reachable. This issue has been fixed. In IPsec tunnel configurations using "0.0.0.0" or an empty field for a local ID or peer ID of type "IP Address", the tunnel was not established. This issue has been fixed.
82461	**OpenVPN changes** Cryptographically weak ciphers are now accepted by default on OpenVPN connections for backwards compatibility with legacy OpenVPN setups. For improved security, support for weak ciphers can be disabled. Client configurations exported with weak ciphers enabled cannot be imported into software versions 4.4 and older. This is intended in order to maintain compatibility with current software versions.
82755	**L2TPv3** In previous versions, a bug in the L2TPv3 implementation prevented tunnels with udp encapsulation to become up. This issue has been fixed.
82897	**OpenVPN** In certain edge conditions, the modification of OpenVPN tunnel settings could hang for a long time and all successive OpenVPN modifications would hang aswell, until the device was rebooted. This issue has been fixed.
82912	**Webserver configuration** Fixed a redirect issue when upgrading to a secure connection. There was no direct security implication.

5 OSS Notice

We inform you that NetModule products may contain in part open source software. We are distributing such open source software to you under the terms of GNU General Public License (GPL)[1], GNU Lesser General Public License (LGPL)[2] or other open source licenses[3].

These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at router@support.netmodule.com.

---

[1]GPLv2 license is available at http://www.gnu.org/licenses/gpl-2.0.txt
[2]LGPL license is available at http://www.gnu.org/licenses/lgpl.txt
[3]OSI licenses (ISC License, MIT License, PHP License v3.0, zlib License) are available at http://opensource.org/licenses

6 Change History

Version	Date	Name	Reason
1.0	Jun 14, 2023	Felix Kopf	Final version

NetModule AG is located at:

Maulbeerstrasse 10
CH-3011 Bern
Switzerland

info@netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

For more information about NetModule AG visit the NetModule website at *www.netmodule.com.*