NET MODULE
Maulbeerstrasse 10
CH-3011 Bern
Switzerland
info@netmodule.com
http://www.netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

Release Note NRSW 4.7.0.100

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.7.0.100. 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-4.7.0.100
Status	Final

Creation:

Role	**Name**
Author	Moritz Rosenthal
Review	Benjamin Amsler

Approval

Role	**Name**
Director Product Development	Benjamin Amsler

1 Release Information

NetModule Router Software:

Version:	**4.7.0.100**
Date:	**Apr 20, 2022**

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

2 New Features

Case-#	Description
59655 **77794**	**CLI improvements** The command line interface now shows active DHCP leases in status output. CLI now shows more detailed information on the current WWAN module state.
69360 **74263** **77886**	**WLAN Pseudo-Bridge** The WLAN Pseudo-Bridge supports Bridging of WLAN client devices without the need for 4-address-frames or Meshing technology by relaying DHCP and broadcast messages.
69372 **78385**	**Wired 802.1X authenticator with optional MAB fallback** Bridged Ethernet interfaces now support 802.1X as authenticator against external radius server.
70464	**PoE port settings** It is now possible to enable or disable PoE per port on NB1810 with PoE support. Also the Ethernet status pages show detailed information on voltage and current drain.
70636	**Change PLMN without global WWAN restart** Changing the allowed PLMN on one WWAN module triggered a restart of all WWAN connections on all modules. This was changed. An ongoing WWAN connection is not interrupted by PLMN change on another connection.
75294	**OSPF improvements** It is now possible to configure an OSPF router ID.
75475 **75937**	**Support for new WWAN modules** The NRSW now supports Telit 5G and LTE modules FN980, LE910C4-EU and LN920A12-WW. Router Hardware dependency has to be considered. The web interface status page shows detailed cell information if link aggregation is used by these modules.
76036	**SDK improvements** It is now possible to install certificates for the MQTT deamon via SDK and CLI.
77165	**Support for Docker in LXC** The LCX container now supports guest systems which run a docker host.
77230	**Increase number of Ethernet WAN links** The maximum number for LAN or VLAN based WAN interfaces was increased to 10.
77339 **77340**	**BGP improvements** It is now possible to configure the router ID for BGP. The address family can now be configured to L2VPN EVPN instead of IPv4-unicast.
77573	**Random certificate key** On initial login from factory state a random key is generated to store generated and uploaded key encrypted internally. In the past a dedicated key had to be configured. This is still possible.
77804	**Number of static multicast routes increased** It is now possible to configure up to 10 static multicast routes.
78085	**GUI improvements** The WWAN configuration via list of known APN does now allow to select IP version for the connection.

3 Security Fixes

The following security relevant issues have been fixed.

Case-#	Description
74452	**Additional HTTP Security Header added to web interface** The HTTP Content-Security-Policy response header whitelists resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
78025 **78026** **78028** **78029** **78030** **78031**	**Security Bug-Fixes for libexpat** The open source library is used in context with ITxPT in our software. CVE-2018-20843 fixes a potential Denail-Of-Service attack. CVE-2019-15903 fixes a potential heap overflow. CVE-2022-22822 to CVE-2022-22827 fix several potential integer overflows. CVE-2021-46143 fixes a potential integer overflow. CVE-2021-45690 fixes an issue with potential left shifts by 29 places or more. CVE-2022-23852 fixes a potential integer overflow.
78103	**Linux kernel security patches** CVE-2022-0492 fixes a missing capabilities check for cgroups.
78106	**Security issues fixed in BusyBox package** CVE-2018-20679 and CVE-2019-5747: An out of bounds read in udhcp server, client and relay may allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. CVE-2018-1000500 and CVE-2021-42374 - CVE-2021-42386: These CVEs have been fixed in the source code even though they did not apply to the NRSW or were only exploitable by users with administrative status which have full access to the device anyway.
78344 **78803**	**OpenSSL security patches** CVE-2021-4160: Actually NRSW was not affected because this applies to MIPS hardware only. Never the less we applied the patch in case we ever adopt our system to this hardware. For existing routers running NRSW on ARM or PPC this should have no impact at all. CVE-2022-0778 fixed possible remote denial of service attack when parsing certificates. In NRSW only users with administrative rights may install certificates. Therefor the severity is considered low.
78954	**CVE-2018-25032 zlib denail of service** The compression library zlib was vulnerable to a memory corruption when compressing input with distant matches. The upstream patches were back-ported to NRSW.

4 Fixes

The following issues and problems have been fixed.

Case-#	Description
60843	**WLAN antenna configuration** The WLAN antenna selection had no effect on recent hardware. This was fixed. Those devices which do not provide the feature do not show the option in the web interface any more.
65823 **74590** **75393** **75394** **75701** **75946** **77099** **77139** **77337** **77487** **77591** **77595** **77596** **77653** **78157** **78477** **78742**	**GUI improvements** With NRSW 4.6 it was not possible any more to add or delete QoS queues from the web interface. This was fixed. The initial password setup did not deny non-ASCII characters in the user password. Never the less these characters were not handled correctly resulting in a device where the user could not log in. This was fixed. Now non-ASCII characters are rejected with an appropriate error message. The tabbing links under System - Settings were broken. This was fixed. If a 3rd party software package was published under more than one license the link to the second license text was broken. This was fixed. The web interface WAN status page did not show IPv6 address. This was fixed. A failure was fixed that prevented to set up ToS based extended routing filters. The web interface showed a misleading message when a new WWAN connection assigned a second SIM card to a WWAN module. The message was corrected. Dead-reckoning settings could not be applied for GNSS modules NEO-M8L with UDR firmware or NEO-M8U. This was fixed in the GUI. Links to support web sites for trouble shooting were updated. Some eUICC profiles could not be imported via GUI interface. This was due to an invalid integrity check of the activation code. This was fixed. A WWAN network Scan always showed results linked to SIM1 even if another SIM was configured and used for the network scan. This was fixed. Not yet applied IPsec tunnel configurations could not be deleted via web interface. This was fixed. An Ethernet WAN link was not removed from the WAN link list if the corresponding Ethernet interface was bridged to another logical LAN interface. This was fixed. The button "Refresh" on the WLAN channel utilization page resulted in a misleading error message. The issue was fixed and now the "Refresh" button works as expected. The system status page did not show the correct system power supply voltage range. The value was changed to meet the requirements from the manual and the specification plate. It was not possible to set client routes while the OpenVPN server was enabled. This was fixed. Some GUI input fields escaped HTML characters twice. This was fixed.
74299	**OpenVPN** Due to an update of openssl, older configurations with ciphers like md5 were no longer accepted which broke backwards compatibility. This issue has been fixed.
74832	**WLAN AP configuration with automatic channel selection could fail** In some situations the WLAN Access-Point with automatic channel selection did not start up correctly due to a timing issue. This was fixed.
74962	**Bridged VLAN blocks broadcast packets** The hardware switch chip drops VLAN tagged broadcast packets if a VLAN is bridged with an Ethernet interface. This was fixed by disabling the HW offload in such situations.
75212	**Missing time zones** The time zones America/Argentina/Buenos_Aires and America/Kentucky/Louisville were missing in the list of supported time zones. This was fixed.
75827	**SNMP v1 broken** With NRSW 4.5 and 4.6 the SNMP server did not answer on SNMP v1 requests any more. This was fixed.

Case-#	Description
75844	**2nd DNS relay service does not work** Configurations with different DNS relay servers for different interfaces did not work. This was fixed.
77270	**OpenVPN generated invalid client configuration files** The client configuration files generated by NRSW contained an invalid protocol entry making it impossible to use them for proper client configuration. This was fixed. You may have to regenerate client configuration files if you faced this problem.
77576	**WLAN dual mode did not show up as WAN interface** If WLAN was configured in dual mode the client connection sometimes was not enabled as new WAN connection. This was fixed.
77725	**WWAN connection broken after switch from 2G-first to 4G-only** It could happen that no WWAN connection came up after switching from 2G-first to 4G only even though both networks were available. This was fixed.
77888	**DHCP requests failed if 802.1X authenticator was enabled** In some setups the DHCP server did not answer on DHCP requests on ports where the 802.1X authenticator was enabled. This was fixed.
78966	**CLI improvements** Sending a techsupport to via email resulted in a crash of the CLI process. This was fixed.
78995	**IP passthrough failed** In some situations IP passthrough failed to propagate the IP settings correctly. This resulted in a reboot loop because the DHCP settings were considered invalid.

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	Apr 20, 2022	Moritz Rosenthal	Final RN

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.*