Release Note NRSW 4.0.0.111

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.0.0.111. It informs on new functionality, corrections and known issues of this software version of NetModule's router series in comparison to the current old-stable release 4.0.0.110.
This release is the last planned release of the 4.0.0 cycle. We recommend to update existing projects to 4.1.0.

Keywords:

NetModule, Software Development, NRSW, Release Note

Document Control:

Document:

Version	1.0
File	NRSW-RN-4.0.0.111
Status	Valid

Creation:

Role	Name
Author	Moritz Rosenthal
Review	Benjamin Amsler

Approval

Role	Name
Director Product Development	Michael Enz

1 Release Information

NetModule Router Software:

Version:	**4.0.0.111**
Date:	**November 19, 2018**

Supported Hardware:

NetModule Router	Hardware Version
NB1600	V1.0 - V3.3
NB2700	V1.0 - V2.7
NB2710	V1.0 - V2.7
NB2800	V1.0 - V1.4
NB3700	V2.0 - V4.3
NB3701	V1.0 - V1.4
NB3710	V2.0 - V4.3
NB3711	V1.0 - V1.4
NB3720	V2.0 - V4.3
NB3800	V1.0 - V1.4

Unsupported Hardware:

NetModule Router
NB800 Series
NB1300 Series
NB1601 Series
NB1800 Series
NB2200 Series
NB2300 Series
NB2500 Series
NB2600 Series

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

2 New Features

Case-#	Description
48684	**Wait for configuration change task to be finished** Changing a configuration setting via CLI or SDK does not block. A new function was implemented to request if all pending tasks have been finished and it is safe to send new configuration change requests.
49268	**Support for new GNSS modules** Added support for new Ublox NEO-M8 modules.
49269	**uBlox TOBY-L2 support** The uBlox Toby-L2 LTE modem is now supported.
53880	**Conversion of configuration version 1.12** Configuration files of version 1.12 can be imported or converted on down grade from newest SW release.

3 Security Fixes

The following security relevant issues have been fixed.

Case-#	Description
52029	**Update of Lighttpd** On release 4.2.0.100 Lighttpd was updated to version 1.4.50. On older releases Security relevant issues were back ported. CVE-2015-3200: Injection of log entries fixed on lighttpd
53324	**Log display in web interface vulnerable to Cross-Site-Scripting (XSS) attack** The web interface which displays the system log was vulnerable to JavaScript XSS attacks. An attacker capable of placing malitious content in the system log could execute JavaScript code in the web browser of the user.
53513	**Security bug fixes on 3rd party SW packages** CVE-2015-3200: Use-after-free fixed in Linux kernel

4 Fixes

The following issues and problems have been fixed.

Case-#	Description
41149	**Roaming failed with Huawei ME909u-521** Devices equipped with Huawei ME909u-521 LTE modules sometimes failed to connect in roaming environment.
49327	**Mismatch between VLAN network settings and DHCP settings triggers reboot** In situations where the VLAN network settings (network address/netmask) did not fit with the DHCP range configured for that network the router would go into reboot. This was fixed. Now the DHCP server on the mis-configured interface will not be started and a warning is given to the user.
49353	**Authorities certificates were not used for all HTTPS downloads** Some functions where data is downloaded from a server the "Authorities" certificates were not used. E.g. it was not possible to update WWAN module firmware from HTTPS.
51090	**SDK improvements** Fixed typo in modification time of files in nb_transfer_list.
51475	**uBlox TOBY-L2 improvements** Clients connected to the LAN side of the router could not communicate to the WAN network, because IP forwarding was disabled. That has been fixed.
51575 53592	**GUI improvements** The interface numbering was wrong during modem firmware update. This has been fixed. Clicking on 'Cancel' in the certificate settings accidentally applied the changes.
52309	**User names starting with 'admin' or 'root' not able to login** Additional users starting with 'admin' or 'root' like 'admin-user' were not able to login after change of administrator password.
52357	**Ping supervision failed on IP pass-through** In IP pass-through the ping supervision failed to contact the server and therefor restarted the router even if the WWAN connection was fine.
52927	**No connection after switching to roaming network** If a router with Huawei ME909 LTE module changes from 3G home network to 4G roaming network it sometimes lost connection and did not recover until back in home network.
53587	**Certificate key handling** Changing the certificate key of the system could fail and leave the system without usable certificate keys. This was fixed.
53608	**Empty user password affected other users** If the setting 'user.0.password' contained an empty string all other users were not able to log in any more. This is not a valid configuration anyway, but it was not intended behavior either and therefor was fixed.

5 ECC conversion

The flash on NB1600, NB2700, NB2710, NB3700, NB3710 and NB3720 provides an automated error correction using ECC. We changed the ECC length from 1-bit ECC to 4-bit ECC which provides better error correction. On first boot after the update was performed the data on the flash is automatically converted to use the new ECC setup. While this conversion is performed the LEDs show a running light for about 30 seconds.

If you switch back to an older software release like 4.0.0 the migration is reverted.

We tested updates and down-grades to and from 4.0.0 and 3.8.0. Updates to or from older versions are not supported. If you run an older release or want to downgrade to an older release or a feature release like 3.8.2 you are advised to migrate via 4.0.0 as an intermediate release.

To revert the migration on downgrade the SPL boot loader release 4.1.0 stays in place. It can be downgraded in a second sofware update process initiated from the target release after the first reboot.

Software updates with recovery images require special attention. You must not use recovery images 4.0.0 and older for systems running 4.1.0 and newer. If you want to use recovery images please contact our support at router@support.netmodule.com.

6 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

7 Change History

Version	Date	Name	Reason
1.0	2018-11-19	rosenthal	Final

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.*