Meriedweg 11
CH-3172 Niederwangen
Switzerland
info@netmodule.com
http://www.netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

Release Note NRSW 4.0.0.108

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.0.0.108. It informs on new functionality, corrections and known issues of the current software version of NetModule's router series.

Keywords:

NetModule, Software Development, NRSW, Release Note

Document Control:

Document:

Version	1.0
File	NRSW-RN-4.0.0.108
Status	Valid

Creation:

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

Approval

Role	**Name**
Director Product Development	Michael Enz

1 Release Information

NetModule Router Software:

Version:	**4.0.0.108**
Date:	**October 25, 2017**

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 - V1.3
NB3710	V2.0 - V4.3
NB3711	V1.0 - V1.3
NB3720	V2.0 - V4.3
NB3800	V1.0 - V1.3

Unsupported Hardware:

NetModule Router
NB1300 Series
NB2200 Series
NB2300 Series
NB2500 Series
NB2600 Series

2 New Features

Case-#	Description
40615	**Firmware Update for Sierra Wireless MC74xx Modems** It is now possible to upgrade the firmware for Sierra MC74xx modems.

3 Fixes

The following issues and problems have been fixed.

Case-#	Description
45729 **45731** **46162**	**OpenVPN Update** CVE-2017-7478: Possible pre-authentication DoS attack on OpenVPN server and client. Attacker must have the TLS authentication key. This was fixed. CVE-2017-7479: An authenticated client could cause a DoS on the server. This was fixed. CVE-2017-7508: A malformed packet could cause a DoS by crashing the OpenVPN server. This was fixed.
46620	**Fixed unstable LTE connection** With one provider, we had bad internet performance with MC7455 under certain circumstances. This was fixed.
46742 **46744** **47291**	**Linux kernel CVEs** CVE-2017-7533 A race condition can lead to local user privilege escalation CVE-2017-1000112 Linux kernel exploitable memory corruption CVE-2017-1000251 Blueborne - remote DoS in Bluetooth subsystem
46847	**Generating and transmitting a techsupport file from SDK timed out** Techsupport files are generated on demand. SDK transmit of techsupport via 'nb_transfer_put' timed out before the file was ready.
46852	**Opening several parallel SSH sessions for user admin fails** When several parallel SSH connections for user admin were open at the same time no more connections would be established. A failure in CLI console memory management was fixed.
47014	**NMEA messages with 'newline' instead of 'carriage-return + newline' after modem reset** If the WWAN/GNSS module was restarted due to ping supervision the GNSS stream provided via TCP was malformed afterwards.
47199	**SDK read from bigger temporary files failed** Due to a misaligned buffer offset reading temporary files bigger than 1024 bytes failed.
47219	**Mount storage from SDK** Fixed an error when trying to mount USB storage from SDK script.
47706	**Possible file system corruption on reboot** There were situations where NB2800 Devices showed file system errors after power cycle. These are recognized recovered automatically now.
47840	**Fixed KRACK attack Wi-Fi issue** A weakness in the Wi-Fi standard itself allows a remote attacker to perform a man-in-the-middle attack to encrypted Wi-Fi connections. This is an attack to Wi-Fi clients and the bug-fix applies only to devices configured as client respectively. If you run an encrypted Wi-Fi in AP mode all clients have to be patched to be invulnerable to this attack (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088).
47894	**dnsmasq update** CVE-2015-3294: Remote attacker could read local process memory and cause DoS. CVE-2017-13704, CVE-2017-14495, CVE-2017-14496: Remote attacker could cause DoS by crashing dnsmasq process. CVE-2017-14491, CVE-2017-14492, CVE-2017-14493: Remote attacker could cause DoS by crashing dnsmasq process and potentially execute code. CVE-2017-14494: Remote attacker could read local process memory. These issues were fixed.

Case-#	Description
47997	**Don’t forward packages of local networks** Packets which belonged to networks of local interfaces were routed over IPsec links, if they were neither originated from nor targeted to the router (iptables FORWARD chain). That was fixed.

4 Known Issues

Items listed here represent minor problems known at release time. These issues will be resolved in a later version.

Case-#	Description

5 Pitfalls

Items listed as pitfalls are potential problems that may arise because of specific environmental conditions.

Case-#	Description
41620	**IPsec IKE Phase2 Defaults** As described, we turned off the automatic fallback to default algorithms in case the peer disagrees about proposals. This might break existing IPsec setups wich have an inconsistent configuration. Please double check that your IPsec configuration is sane before performing an update.
45052	**Dropping ICMP Packets with Timestamps** Please note that any ICMP packets with timestamps are now dropped which may break applications. Using timestamps is discouraged and therefore usually not wide-spread. However, please disable ICMP timestamps in case you face any issues.

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	2017-10-25	amsler	Final

NetModule AG is located at:

Meriedweg 11
CH-3172 Niederwangen
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.*