

# 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:

<b>Document:</b>	<b>Version</b>	1.0
	<b>File</b>	NRSW-RN-4.0.0.108
	<b>Status</b>	Valid
<b>Creation:</b>	<b>Role</b>	<b>Name</b>
	Author	Benjamin Amsler
	Review	Moritz Rosenthal
<b>Approval</b>	<b>Role</b>	<b>Name</b>
	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

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



---

## 2 New Features

---

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

---

### 3 Fixes

The following issues and problems have been fixed.

Case-#	Description
<b>45729</b>	<b>OpenVPN Update</b>
<b>45731</b>	CVE-2017-7478: Possible pre-authentication DoS attack on OpenVPN server and client. Attacker must have the TLS authentication key. This was fixed.
<b>46162</b>	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.
<b>46620</b>	<b>Fixed unstable LTE connection</b> With one provider, we had bad internet performance with MC7455 under certain circumstances. This was fixed.
<b>46742</b>	<b>Linux kernel CVEs</b>
<b>46744</b>	CVE-2017-7533 A race condition can lead to local user privilege escalation
<b>47291</b>	CVE-2017-1000112 Linux kernel exploitable memory corruption CVE-2017-1000251 Blueborne - remote DoS in Bluetooth subsystem
<b>46847</b>	<b>Generating and transmitting a techsupport file from SDK timed out</b> Techsupport files are generated on demand. SDK transmit of techsupport via 'nb_transfer_put' timed out before the file was ready.
<b>46852</b>	<b>Opening several parallel SSH sessions for user admin fails</b> 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.
<b>47014</b>	<b>NMEA messages with 'newline' instead of 'carriage-return + newline' after modem reset</b> If the WWAN/GNSS module was restarted due to ping supervision the GNSS stream provided via TCP was malformed afterwards.
<b>47199</b>	<b>SDK read from bigger temporary files failed</b> Due to a misaligned buffer offset reading temporary files bigger than 1024 bytes failed.
<b>47219</b>	<b>Mount storage from SDK</b> Fixed an error when trying to mount USB storage from SDK script.
<b>47706</b>	<b>Possible file system corruption on reboot</b> There were situations where NB2800 Devices showed file system errors after power cycle. These are recognized recovered automatically now.
<b>47840</b>	<b>Fixed KRACK attack Wi-Fi issue</b> 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).
<b>47894</b>	<b>dnsmasq update</b> 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	<b>Don't forward packages of local networks</b> 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
<b>41620</b>	<p><b>IPsec IKE Phase2 Defaults</b></p> <p>As described, we turned off the automatic fallback to default algorithms in case the peer disagrees about proposals. This might break existing IPsec setups with an inconsistent configuration. Please double check that your IPsec configuration is sane before performing an update.</p>
<b>45052</b>	<p><b>Dropping ICMP Packets with Timestamps</b></p> <p>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.</p>

## 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)<sup>1</sup>, GNU Lesser General Public License (LGPL)<sup>2</sup> or other open source licenses<sup>3</sup>.

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](mailto:router@support.netmodule.com).

---

<sup>1</sup>GPLv2 license is available at <http://www.gnu.org/licenses/gpl-2.0.txt>

<sup>2</sup>LGPL license is available at <http://www.gnu.org/licenses/lgpl.txt>

<sup>3</sup>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

### Copyright © 1998 - 2017 NetModule AG; All rights reserved

This document contains proprietary information of NetModule AG. No part of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and is protected by patent law. This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated in any language or computer language without the prior written permission of NetModule AG.

The information in this document is subject to change without notice. NetModule AG makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this information. This document may contain information about third party products or processes. This third party information is out of influence of NetModule AG therefore NetModule AG shall not be responsible for the correctness or legitimacy of this information. If you find any problems in the documentation, please report them in writing by email to [info@netmodule.com](mailto:info@netmodule.com) at NetModule AG.

While due care has been taken to deliver accurate documentation, NetModule AG does not warrant that this document is error-free.

"NetModule AG" and "NetModule Router" are trademarks and the NetModule logo is a service mark of NetModule AG.

All other products or company names mentioned herein are used for identification purposes only, and may be trademarks or registered trademarks of their respective owners.

The following description of software, hardware or process of NetModule AG or other third party provider may be included with your product and will be subject to the software, hardware or other license agreement.

NetModule AG is located at:

Meriedweg 11  
 CH-3172 Niederwangen  
 Switzerland

[info@netmodule.com](mailto: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](http://www.netmodule.com).