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 4.7.0.101

## Project Name: NRSW

## Abstract:

This document represents the release note for NetModule Router Software 4.7.0.101. 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** | 1.1 |
| **File** | NRSW-RN-4.7.0.101 |
| **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: | **4.7.0.101** |
| Date: | **Sep 30, 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 |
|---|---|
| **66500** | **Support for ECC Certificates and Keys**<br>Elliptic curve cryptography certificates and keys are supported by NRSW now. |
| **78183** | **Update of 3rd party open source packages**<br>The tcpdump debug tool was updated to version 4.9.3. |
| **78320** | **Update of libidn2**<br>System library libidn2 was updated to version 2.3.2. |
| **79405** | **SSL certificate generation**<br>Use random serial numbers for generated SSL certificates. |
| **79550** | **Adjustment tranmit power and antenna gain**<br>The range of TX power and antenna gain settings has been restricted for TI wl18xx based products NB800, NG800 and NB1601 to ensure RSE compliance is met under all conditions. It is only possible to reduce the transmit power of the module to 10 dBm. Additional antenna gain reduces the margin accordingly. |
| **79906** | **IPsec improvements**<br>Local and remote IKE port are now configurable. |
| **79967** | **Scheduled WWAN module restart**<br>Some customers faced problems with stationary devices which did sporadically disconnect from the base station. A nightly reset was introduced. This is enabled by default for affected modules, but can be disabled if not required. |

## 3 Security Fixes

The following security relevant issues have been fixed.

| Case-# | Description |
|---|---|
| **78063** | **CVE-2018-17937: Stack based buffer overflow in gpsd**<br>A stack-based buffer overflow was discovered in gpsd on port 2947/TCP or crafted JSON inputs. This might result in Crashes or execution of injected code. |
| **78095** | **Security issues in Mosquitto MQTT library**<br>CVE-2021-34431: If an authenticated client that had connected with MQTT v5 sent a crafted CONNECT message to the broker a memory leak would occur, which could be used to provide a DoS attack against the broker.<br>CVE-2021-34432: The server will crash if the client tries to send a PUBLISH packet with topic length = 0.<br>CVE-2021-41039: An MQTT v5 client connecting with a large number of user-property properties could cause excessive CPU usage, leading to a loss of performance and possible denial of service. |
| **78096** | **Security patches for gmp system library**<br>CVE-2021-43618: GNU Multiple Precision Arithmetic Library (GMP) has an integer overflow and resultant buffer overflow via crafted input, leading to a segmentation fault. |
| **78189** | **Security issues in the D-Bus**<br>CVE-2020-12049: A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients. |
| **78190** | **Security patches for strongswan IPsec**<br>CVE-2021-41990: The gmp plugin has a remote integer overflow via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur.<br>CVE-2021-41991: The in-memory certificate cache has a remote integer overflow upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. Remote code execution might be a slight possibility.<br>CVE-2021-45079: A malicious responder can send an EAP-Success message too early without actually authenticating the client and (in the case of EAP methods with mutual authentication and EAP-only authentication for IKEv2) even without server authentication. |
| **78314** | **Security patches for libpcre**<br>CVE-2020-14155: An integer overflow via a large number after a special substring may occur. |
| **78336** | **Security patches for lldpd**<br>CVE-2020-27827: Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service. |
| **78342** | **Security patches for LXC**<br>CVE-2019-5736: A malicious container may execute code on the host system if the administrator connects to the running container via LXC, |
| **78345** | **Security patches for dnsmasq**<br>CVE-2021-3448: When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this vulnerability is to data integrity. |

| Case-# | Description |
|---|---|
| **78346** | **Security patches for Avahi**<br>CVE-2021-3468: A flaw was found in avahi. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. The highest threat from this vulnerability is to the availability of the avahi service, which becomes unresponsive after this flaw is triggered. |
| **78347** | **Security patches for Dropbear SSH**<br>CVE-2020-36254: The scp tool in Dropbear before 2020.79 mishandled the filename of . or an empty filename. |
| **78349** | **Security patches for OpenVPN**<br>CVE-2020-11810: An attacker can inject a data channel v2 (P_DATA_V2) packet using a victim's peer-id. Normally such packets are dropped, but if this packet arrives before the data channel crypto parameters have been initialized, the victim's connection will be dropped. This requires careful timing due to the small time window (usually within a few seconds) between the victim client connection starting and the server PUSH_REPLY response back to the client. This attack will only work if Negotiable Cipher Parameters (NCP) is in use. In NRSW NCP is not used and might only be configured via users expert mode file configuration.<br>CVE-2020-15078: A remote attacker may bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks. In NRSW deferred authentication is not used and might only be configured via users expert mode file configuration. |
| **79271**<br>**79272** | **Security issues in net-snmp**<br>CVE-2020-15862: Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root. SNMP write access to the MIB requires administrative access to NRSW anyway.<br>CVE-2020-15861: Due to incorrect handling of symlinks sensitive data could be disclosed. |
| **79435**<br>**79436**<br>**79437**<br>**79457** | **Security patch for ncurses system library**<br>CVE-2019-17594: Heap based buffer overflow may lead to denial of service or be a vector for code injection.<br>CVE-2019-17595: Heap based buffer overflow may lead to denial of service or be a vector for code injection.<br>CVE-2021-39537: Heap based buffer overflow may lead to denial of service or be a vector for code injection.<br>CVE-2022-29458: Out-of-bounds read and segmentation violation may result in denial of service. |
| **79524**<br>**79527**<br>**79528** | **Security patches for glib system library**<br>CVE-2020-35457: Fix for potential integer overflow which might result in out-of-bounds write,<br>CVE-2021-28153: When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)<br>CVE-2019-12450: A file copy may not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used. |
| **79602**<br>**79618**<br>**80276** | **Security issues in the PHP scripting language**<br>CVE-2015-9253: An authenticated administrative user could cause a denial of service to the PHP interface by malformed PHP script.<br>CVE-2019-9637: Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling non administrative users to access the data. In NRSW unauthorized users do not have shell or direct file system access.<br>CVE-2019-11048: Possible denial on service due to insufficient handling of upload file names. On NRSW only authenticated administrative users are able to upload files. |

| Case-# | Description |
|---|---|
| **79924** | **Security patches for libssh2 system library**<br>In libssh2 an integer overflow could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. |
| **80004**<br>**80005**<br>**80006**<br>**80007** | **Security patches for libyang used by FRRouting**<br>CVE-2021-28902: Possible NULL pointer dereference could lead to program crash and denial of service.<br>CVE-2021-28906: Possible NULL pointer dereference could lead to program crash and denial of service.<br>CVE-2021-28903: Possible denial of service by uncaught infinite recursion.<br>CVE-2021-28904: Possible NULL pointer dereference could lead to program crash and denial of service.<br>CVE-2021-28905: Possible DoS by malformed assert on eventually NULL object. |
| **80018**<br>**80019** | **Security issues fixed in U-Boot**<br>CVE-2022-30790: Fixed remote execution in U-Boot. This can only be exploited if the IP stack in U-Boot is initialized. This does not happen on regular boot. The IP stack is started only if an authenticated user interrupts the boot via serial interface or if the recovery boot procedure was started via physical reset button. In both cases the local user has full access anyway.<br>CVE-2022-30552: buffer overflow |
| **80119** | **Security patches for the kernel's performance events functionality**<br>CVE-2022-1729: A use-after-free could allow a local user to crash the system. |
| **80130**<br>**80132**<br>**80133**<br>**80134** | **Security issues in GnuTLS library used by radius client**<br>CVE-2020-11501: GnuTLS uses incorrect cryptography for DTLS. The DTLS client always uses 32 zero bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.<br>A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.<br>CVE-2021-20231: A potential use after free may lead to memory corruption.<br>CVE-2021-20232: A potential use after free may leed to memory corruption. |

| Case-# | Description |
|---|---|
| **80579** | **Security patches for Kernel 4.19.163**<br>CVE-2020-27825: There was a race problem in trace_open and resize of cpu buffer may cause a denial of service problem (DOS).<br>CVE-2021-3347: PI futexes have a kernel stack use-after-free during fault handling.<br>CVE-2021-21781: An information disclosure vulnerability exists in the ARM SIGPAGE functionality. A userland application can read the contents of the sigpage, which can leak kernel memory contents.<br>CVE-2021-29650: The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value.<br>CVE-2021-22555: A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c.<br>CVE-2020-29374: An issue related to mm/gup.c and mm/huge_memory.c. The get_user_pages (aka gup) implementation, when used for a copy-on-write page, does not properly consider the semantics of read operations.<br>CVE-2021-32399: net/bluetooth/hci_request.c has a race condition for removal of the HCI controller.<br>CVE-2021-33034: net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan.<br>CVE-2021-3564: A flaw double-free memory corruption in the HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device.<br>CVE-2021-3573: A use-after-free in function hci_sock_bound_ioctl() which triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info()<br>CVE-2021-35039: kernel/module.c mishandles Signature Verification. Without CONFIG_MODULE_SIG, verification that a kernel module is signed, for loading via init_module, does not occur for a module.sig_enforce=1 command-line argument.<br>CVE-2021-45486: In the IPv4 implementation net/ipv4/route.c has an information leak because the hash table is very small.<br>CVE-2021-33909: fs/seq_file.c does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write.<br>CVE-2021-45485: In the IPv6 implementation net/ipv6/output_core.c has an information leak because of certain use of a too small hash table.<br>CVE-2021-0920: In unix_scm_to_skb of af_unix.c, there is a possible use after free bug due to a race condition.<br>CVE-2021-3732: In OverlayFS subsystem wheBVre a local attacker can abuse a logic bug in the overlayfs code which can inadvertently reveal files hidden in the original mount.<br>CVE-2021-39633: In gre_handle_offloads of ip_gre.c, there is a possible page fault due to an invalid memory access.<br>CVE-2021-40490: A race condition was discovered in Bext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem.<br>CVE-2022-20141: In ip_check_mc_rcu of igmp.c, there is a possible use after free due to improper locking.<br>CVE-2021-37159: hso_free_net_device in drivers/net/usb/hso.c calls unregister_netdev without checking for the NETREG_REGISTERED state.<br>CVE-2021-4203: A use-after-free read flaw was found in sock_getsockopt() in net/core/sock.c due to SO_PEERCRED and SO_PEERGROUPS race with listen() (and connect()).<br>CVE-2021-20317: A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c.<br>CVE-2021-20321: A race condition accessing file object in the Linux kernel OverlayFS subsystem was found in the way users do rename in specific way with OverlayFS.<br>CVE-2022-0644: vfs: check fd has read access in kernel_read_file_from_fd()<br>CVE-2021-20322: A flaw in the processing of received ICMP errors (ICMP fragment needed and ICMP redirect) allowed to quickly scan open UDP ports and effectively bypass the source port UDP randomization.<br>CVE-2021-3752: A use-after-free flaw was found in the Linux kernel's Bluetooth subsystem in the way user calls connect to the socket and disconnect simultaneously due to a race condition. |

| Case-# | Description |
|---|---|
| **80579** | **Security patches for Kernel 4.19.163**<br>CVE-2021-4083: A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition.<br>CVE-2021-39698: In aio_poll_complete_work of aio.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed.<br>CVE-2020-36322: A flaw in FUSE filesystem fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash.<br>CVE-2022-1678: An improper update of sock reference in TCP pacing can lead to memory/netns leak, which can be used by remote clients.<br>CVE-2022-20008: In mmc_blk_read_single of block.c, there is a possible way to read kernel heap memory due to uninitialized data with no additional execution privileges needed.<br>CVE-2022-23960: ARM: report Spectre v2 status through sysfs<br>CVE-2022-1016: netfilter: nf_tables: initialize registers in nft_do_chain() to avoid stack leak into userspace.<br>CVE-2022-27666: A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects.<br>CVE-2021-4197: An unprivileged write to the file handler flaw in the Linux kernel's control groups and namespaces subsystem was found in the way users have access to some less privileged process.<br>CVE-2022-1011: A use-after-free flaw was found in the FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem.<br>CVE-2022-1353: A vulnerability in the pfkey_register function in net/key/af_key.c allows a local, unprivileged user to gain access to kernel memory.<br>CVE-2022-30594: The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.<br>CVE-2022-29581: Improper Update of Reference Count vulnerability in net/sched allows local attacker to cause privilege escalation to root.<br>CVE-2022-1729: A race condition in perf_event_open leads to privilege escalation<br>CVE-2022-0494: A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c.<br>CVE-2022-1012: hash output truncated to 32 bits when using SipHash in place of MD5 for port offset calculation.<br>CVE-2022-1184: ext4: Verify dir block before splitting so that the splitting code does not access memory it should not.<br>CVE-2022-32296: The kernel allowed TCP servers to identify clients by observing what source ports are used. |

## 4 Fixes

The following issues and problems have been fixed.

| Case-# | Description |
|---|---|
| **77213**<br>**78812**<br>**79565**<br>**80302** | **GUI improvements**<br>Since 4.6.0.100 the "Continue" button was missing in the web configuration interface. This was fixed.<br>VLAN based WAN interfaces configuration was not properly propagated to the configuration since 4.6.0.100. This was fixed. Configuration from older releases were displayed incorrectly, but worked as expected.<br>The web interface always showed the EID of eUICC connected to Mobile1 even when asked for a SIM connected to Mobile2. This was fixed.<br>A VLAN WAN link remained in the list of WAN links when the underlying VLAN interface was removed. |
| **77532** | **SIM PUK handling improved**<br>With multiple SIMs installed it could happen that wrong PUK settings were not recognized resulting in too many attempts to apply the wrong PUK. This would have resulted in SIM in state PUK2 needed or permanently locked. This was found in internal review and fixed. |
| **78639** | **Firewall rules applied incorrectly**<br>Forwarding firewall rules for IPv4 were applied twice with direction in instead of once direction in and once direction out. This was fixed. |
| **78801** | **IPsec improvements**<br>Depending on the configuration the expert mode files generated on the server for clients had an invalid syntax. This was fixed. |
| **79185** | **Modem firmware update**<br>On PowerPC based platforms with release versions 4.5.0.10x and 4.6.0.10x, the firmware for TOBY-L2 modems could not be updated. This issue has been fixed. |
| **79484** | **Openvpn AUTH FAILED can lead to reboot**<br>In certain cases, failed Openvpn authentication leads to a reboot. This was fixed. |
| **79574** | **SDK improvements**<br>Outgoing voice calls could not be started from SDK scripts. This was fixed. |
| **79662** | **Short ethernet frames padded incorrectly on NB800**<br>Short ethernet frames were padded to 64 bytes instead of correct length of 60 bytes. |
| **79835** | **LTE requires 2nd antenna**<br>It was possible to select the number of antennas in the LTE setup. Never the less the LTE standard makes the 2nd antenna mandatory for background-scans. Therefor this feature was discontinued. |
| **79975** | **WLAN mesh station list empty**<br>On NB800, NB1601 and NG800 the list of known WLAN mesh stations showed no devices since NRSW 4.5.0.100. This was fixed. |
| **80067** | **CLI improvements**<br>The product type of NB2810 did not show up correctly in cli status. This was fixed. |
| **80456** | **Missing entries in SNMP vendor MIB file**<br>Traps for POE status changes were missing in the vendor MIB file. This was fixed. |
| **81086** | **IPsec and firewall interaction**<br>In previous releases, for IPsec tunnels with peer-address 0.0.0.0, traffic has been filtered out by the firewall erroneously. This issue has been fixed. |
| **81166** | **Changing the certificate passphrase did not work correctly**<br>If the certificate passphrase was changed via GUI or due to a configuration update the keys and certificates were not changed correctly. This resulted in problems when generating new certificates in the GUI or in services relying on the existing certificates not to function correct any more. This issue was fixed. |

## 5 Known Issues

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

| Case-# | Description |
|---|---|
| **81316** | **WWAN connections without DNS provider fail to connect**<br>Since NRSW 4.6.0.100 it is mandatory that a DNS provider is pushed by the network. This is not the case in some private APN networks and devices with WWAN modules from Ciellient, Sierra Wireless, SIMCOM or Telit were able to connect without DNS with older NRSW releases. The old behavior will be restored with next releases, |
| **81609** | **Broken OpenVPN after update**<br>Some existing OpenVPN configurations in the field broke during the software update process. As this might have impact on the connectivity of existing solutions we revoked the release and will provide a bugfix release. |

## 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 |
|---|---|---|---|
| 1.1 | Sep 30, 2022 | Moritz Rosenthal | Add information on Case 81609 |
| 1.0 | Sep 15, 2022 | Moritz Rosenthal | Final document |



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.*