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 4.3.0.117

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.3.0.117. 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-4.3.0.117
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:	**4.3.0.117**
Date:	**Sep 30, 2022**

Supported Hardware:

NetModule Router	Hardware Version
NB800	V2.0 - V2.2
NB1600	V1.0 - V3.3
NB1601	V1.0 - V1.6
NB1800	V2.4 - V2.6
NB1810	V2.4 - V2.6
NB2700	V1.0 - V2.7
NB2710	V1.0 - V2.7
NB2800	V1.0 - V1.4
NB3700	V2.0 - V4.4
NB3701	V1.0 - V1.10
NB3710	V2.0 - V4.3
NB3711	V1.0 - V1.5
NB3720	V2.0 - V4.3
NB3800	V1.0 - V1.10

Unsupported Hardware:

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

2 New Features

Case-#	Description
65512	**GUI improvements** To configure local keys and certificates it is mandatory to define a password for key encryption. If you did not do that an error message appeared that was not very helpful. The error message was improved.
78183	**Update of 3rd party open source packages** The tcpdump debug tool was updated to version 4.9.3.
79967	**Scheduled WWAN module restart** 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
69102	**PHP security issues** CVE-2018-10545: Dumpable FPM child processes allow bypassing opcache access controls
78063	**CVE-2018-17937: Stack based buffer overflow in gpsd** 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.
78096	**Security patches for gmp system library** 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.
78314 **79156** **79157** **79158** **79159**	**Security patches for libpcre** CVE-2020-14155: An integer overflow via a large number after a special substring may occur. CVE-2017-6004: A crafted regular expression may cause a denial of service (out-of-bounds read and application crash). CVE-2015-5073: An attacker may cause a denial of service (crash) or obtain sensitive information from heap memory via a crafted regular expression. CVE-2015-3217: Possible denial of service (stack-based buffer overflow) via a crafted regular expression. CVE-2016-3191: Possible denial of service (stack-based buffer overflow) via a crafted regular expression.
78336	**Security patches for lldpd** 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** CVE-2019-5736: A malicious container may execute code on the host system if the administrator connects to the running container via LXC,
78345 **79103**	**Security patches for dnsmasq** 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. CVE-2019-14834: A memory leak allowed remote attackers to cause a denial of service (memory consumption) via vectors involving DHCP response creation.
78346	**Security patches for Avahi** 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 **79100**	**Security patches for Dropbear SSH** CVE-2020-36254: The scp tool in Dropbear before 2020.79 mishandled the filename of . or an empty filename. CVE-2019-12953: Dropbear had an inconsistent failure delay that may lead to revealing valid usernames.

Case-#	Description
78349	**Security patches for OpenVPN** 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. 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 **79272** **79273** **79274**	**Security issues in net-snmp** 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. CVE-2020-15861: Due to incorrect handling of symlinks sensitive data could be disclosed. CVE-1018-18066: A NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service. CVE-1018-18066: A NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
79435 **79436** **79437** **79457**	**Security patch for ncurses system library** CVE-2019-17594: Heap based buffer overflow may lead to denial of service or be a vector for code injection. CVE-2019-17595: Heap based buffer overflow may lead to denial of service or be a vector for code injection. CVE-2021-39537: Heap based buffer overflow may lead to denial of service or be a vector for code injection. CVE-2022-29458: Out-of-bounds read and segmentation violation may result in denial of service.
79524 **79527** **79528**	**Security patches for glib system library** CVE-2020-35457: Fix for potential integer overflow which might result in out-of-bounds write, 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.) 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 **79618** **80276**	**Security issues in the PHP scripting language** CVE-2015-9253: An authenticated administrative user could cause a denial of service to the PHP interface by malformed PHP script. 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. 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
79917 **79918** **79919** **79920** **79921** **79922** **79923** **79924**	**Security patches for libssh2 system library** CVE-2015-1782: Remote servers can cause a denial of service (crash) or have other unspecified impact via crafted length values in an SSH_MSG_KEXINIT packet. CVE-2016-0787: The diffie_hellman_sha256 function in libssh2 improperly truncates secrets to 128 or 256 bits, which makes it easier for man-in-the-middle attackers to decrypt or intercept SSH sessions. CVE-2019-3855: An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. CVE-2019-3856: An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. CVE-2019-3857: An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. CVE-2019-3858: An out of bounds read flaw was discovered in libssh2 before when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. CVE-2019-3859: An out of bounds read flaw was discovered in libssh2 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. CVE-2019-3860: An out of bounds read flaw was discovered in libssh2 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. CVE-2019-3861: An out of bounds read flaw was discovered in libssh2 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. CVE-2019-3862: An out of bounds read flaw was discovered in libssh2 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. CVE-2019-3863: A flaw was found in libssh2. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error. 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.
80077	**Security patches for UPX library used by strace debug utility** Integer overflow might result in denial of service or code injection.
80117	**Linux kernel security patches** CVE-2022-32981: The Linux kernel for powerpc 32-bit has a buffer overflow in the handling of ptrace PEEKUSER/POKEUSER when accessing floating point registers.
80119	**Security patches for the kernel's performance events functionality** CVE-2022-1729: A use-after-free could allow a local user to crash the system.

Case-#	Description
80559	**Security patches for strongswan IPsec** CVE-2017-9022: The gmp plugin does not properly validate RSA public keys, which allows remote peers to cause a denial of service (floating point exception and process crash) via a crafted certificate. CVE-2017-9023: The ASN.1 parser improperly handles CHOICE types when the x509 plugin is enabled, which allows remote attackers to cause a denial of service (infinite loop) via a crafted certificate. CVE-2017-11185: The gmp plugin allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted RSA signature. CVE-2018-5388: A missing packet length check could allow a buffer underflow, which may lead to resource exhaustion and denial of service while reading from the socket. CVE-2018-10811: Missing Initialization of a Variable allows Remote Denial of Service. CVE-2018-16151: The RSA implementation does not reject excess data after the encoded algorithm OID during PKCS signature verification. A remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication. CVE-2018-16152: The RSA implementation based on GMP does not reject excess data during PKCS signature verification. Consequently, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication. CVE-2018-17540: The gmp plugin has a Buffer Overflow via a crafted certificate. 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. 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.

Case-#	Description
80581	**Security patches for Kernel 4.19.30** CVE-2019-3459: A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. CVE-2019-3460: A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1. CVE-2019-11599: The coredump implementation does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service. CVE-2019-9857: The function inotify_update_existing_watch() in fs/notify/inotify/inotify_user.c neglects to call fsnotify_put_mark() with IN_MASK_CREATE after fsnotify_find_mark(), which will cause a memory leak leading to a denial of service. CVE-2019-10125: In aio_poll() in fs/aio.c a file may be released by aio_poll_wake() if an expected event is triggered immediately (e.g., by the close of a pair of pipes) after the return of vfs_poll(), and this will cause a use-after-free. CVE-2019-11487: The Linux kernel allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. It can occur with FUSE req CVE-2019-18805: There is a net/ipv4/tcp_input.c signed integer overflow in tcp_ack_update_rtt() when userspace writes a very large integer to /proc/sys/net/ipv4/tcp_min_rtt_wlen, leading to a denial of service. CVE-2019-20054: There is a NULL pointer dereference in drop_sysctl_table() in fs/proc/proc_sysctl.c, related to put_links. CVE-2019-11477: TCP_SKB_CB(skb)->tcp_gso_segs has an integer overflow when handling TCP Selective Acknowledgments (SACKs) leading to a denial of service. CVE-2019-11478: The TCP retransmission queue implementation in tcp_fragment could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences leading to a denial of service. CVE-2019-11479: The default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced leading to a denial of service. CVE-2019-11833: fs/ext4/extents.c does not zero out the unused memory region in the extent tree block allowing reading of uninitialized data in the filesystem. CVE-2019-12614: There is an unchecked kstrdup of prop->name, which might allow an attacker to cause a denial of service. CVE-2019-13272: ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access. CVE-2019-15666: There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause denial of service. CVE-2019-19332: A setxattr operation, after a mount of a crafted ext4 image, can cause a slab-out-of-bounds write access because of an ext4_xattr_set_entry use-after-free in fs/ext4/xattr.c when a large old_size value is used in a memset call. CVE-2019-19447: Mounting a crafted ext4 filesystem image, performing some operations, and unmounting can lead to a use-after-free. CVE-2019-19530: There is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/class/cdc-acm.c driver CVE-2019-19537: There is a race condition bug that can be caused by a malicious USB device in the USB character device driver layer. CVE-2019-19767: Ext4_expand_extra_isize has demonstrated use-after-free errors in __ext4_expand_extra_isize and ext4_xattr_set_entry, related to fs/ext4/inode.c and fs/ext4/super.c CVE-2019-25045: The XFRM subsystem has a use-after-free, related to an xfrm_state_fini panic. CVE-2019-5108: Exploitable mac80211 vulnerability by triggering AP to send IAPP location updates for stations before the required authentication process has completed. This could lead to different denial-of-service scenarios CVE-2019-9506: The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation.

Case-#	Description
80581	**Security patches for Kernel 4.19.30** CVE-2020-0305: In cdev_get of char_dev.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. CVE-2020-0427: In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. CVE-2020-0466: In do_epoll_ctl and ep_loop_check_proc of eventpoll.c, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. CVE-2020-10135: In Bluetooth BR/EDR Core Specification v5.2 and earlier may allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. CVE-2020-10720: A flaw in GRO allows an attacker with local access to crash the system. CVE-2020-10732: This flaw in the implementation of Userspace core dumps allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data. CVE-2020-10757: A flaw in the way mremap handled DAX Huge Pages allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system. CVE-2020-12114: A pivot_root race condition in fs/namespace.c allows local users to cause a denial of service (panic) by corrupting a mountpoint reference counter. CVE-2020-12351: Improper input validation in L2CAP may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. CVE-2020-12464: Usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference. CVE-2020-14314: A memory out-of-bounds read flaw with the ext3/ext4 file system in the way it accesses a directory with broken indexing. CVE-2020-14386: A memory corruption flaw in net/packet can be exploited to gain root privileges from unprivileged processes. CVE-2020-15436: Use-after-free vulnerability in fs/block_dev.c allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field. CVE-2020-15437: A NULL pointer dereference in drivers/tty/serial/8250/8250_core.c allows local users to cause a denial of service by using the p->serial_in pointer which uninitialized. CVE-2020-16166: A flwa in random32 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG. CVE-2020-24490: Improper buffer restrictions in BlueZ may allow an unauthenticated user to potentially enable denial of service via adjacent access. CVE-2020-25285: A race condition between hugetlb sysctl handlers in mm/hugetlb.c could be used by local attackers to corrupt memory, cause a NULL pointer dereference. CVE-2020-25705: A flaw in ICMP packets may allow an attacker to quickly scan open UDP ports. This flaw allows an off-path remote attacker to effectively bypass source port UDP randomization. CVE-2020-27066: In xfrm6_tunnel_free_spi of net/ipv6/xfrm6_tunnel.c, there is a possible use after free due to improper locking. CVE-2020-29660: A locking inconsistency issue in the tty subsystem drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID. CVE-2020-29661: A locking issue in the tty subsystem drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP. CVE-2020-35508: A race condition and incorrect initialization of the process id int the child/parent process identification handling while filtering signal handlers. CVE-2020-36386: Net/bluetooth/hci_event.c has a slab out-of-bounds read in hci_extended_inquiry_result_evt. CVE-2020-8428: Fs/namei.c has a may_create_in_sticky use-after-free, which allows local users to cause a denial of service (OOPS) or possibly obtain sensitive information from kernel memory. CVE-2020-8648: There is a use-after-free vulnerability in the n_tty_receive_buf_common function in drivers/tty/n_tty.c. CVE-2021-0342: In tun_get_user of tun.c, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges required.

Case-#	Description
80581	**Security patches for Kernel 4.19.30** CVE-2021-0605: In pfkey_dump of af_key.c, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure. CVE-2021-1048: In ep_loop_check_proc of eventpoll.c, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege. CVE-2021-3715: A flaw was found in the "Routing decision" classifier in the Traffic Control networking subsystem in the way it handled changing of classification filters, leading to a use-after-free condition. CVE-2021-39634: In fs/eventpoll.c, there is a possible use after free. This could lead to local escalation of privilege. CVE-2020-27825: There was a race problem in trace_open and resize of cpu buffer may cause a denial of service problem (DOS). CVE-2021-3347: PI futexes have a kernel stack use-after-free during fault handling. 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. 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. CVE-2021-22555: A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. 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. CVE-2021-32399: net/bluetooth/hci_request.c has a race condition for removal of the HCI controller. CVE-2021-33034: net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan. 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. 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() 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. CVE-2021-45486: In the IPv4 implementation net/ipv4/route.c has an information leak because the hash table is very small. CVE-2021-33909: fs/seq_file.c does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write. 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. 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. 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. CVE-2021-39633: In gre_handle_offloads of ip_gre.c, there is a possible page fault due to an invalid memory access. CVE-2021-40490: A race condition was discovered in Bext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem. CVE-2022-20141: In ip_check_mc_rcu of igmp.c, there is a possible use after free due to improper locking. CVE-2021-37159: hso_free_net_device in drivers/net/usb/hso.c calls unregister_netdev without checking for the NETREG_REGISTERED state. 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()). CVE-2021-20317: A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. 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.

Case-#	Description
80581	**Security patches for Kernel 4.19.30** CVE-2022-0644: vfs: check fd has read access in kernel_read_file_from_fd() 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. 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. 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. 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. CVE-2020-36322: A flaw in FUSE filesystem fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. 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. 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. CVE-2022-23960: ARM: report Spectre v2 status through sysfs CVE-2022-1016: netfilter: nf_tables: initialize registers in nft_do_chain() to avoid stack leak into userspace. 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. 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. 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. 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. CVE-2022-30594: The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag. CVE-2022-29581: Improper Update of Reference Count vulnerability in net/sched allows local attacker to cause privilege escalation to root. CVE-2022-1729: A race condition in perf_event_open leads to privilege escalation CVE-2022-0494: A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c. CVE-2022-1012: hash output truncated to 32 bits when using SipHash in place of MD5 for port offset calculation. CVE-2022-1184: ext4: Verify dir block before splitting so that the splitting code does not access memory it should not. 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
75029	**GUI improvements** Web server provided PHP file for download instead of showing an appropriate error message after too many login attempts.
77532	**SIM PUK handling improved** 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.
78801	**IPsec improvements** Depending on the configuration the expert mode files generated on the server for clients had an invalid syntax. This was fixed.
79574	**SDK improvements** Outgoing voice calls could not be started from SDK scripts. This was fixed.
79662	**Short ethernet frames padded incorrectly on NB800** Short ethernet frames were padded to 64 bytes instead of correct length of 60 bytes.
81166	**Changing the certificate passphrase did not work correctly** 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
81609	**Broken OpenVPN after update** 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 ECC conversion

The flash on NB1600, NB2700, NB2710, NB3700, NB3710 and NB3720 provides an automated error correction using ECC. With release 4.1.0.100 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.

7 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

8 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.*