M!DGE/MG102i Release notes

Firmware version 4.0.40.xxx

Release 4.0.40.109
2018-02-27

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

Fixes

SSH server certificate download failed
The certificates which were provided for download from the web GUI were not in the right format to reinstall them into another device. This was fixed.

GUI improvements
Special characters like '@' or '!' were not allowed as APN password in web interface. This was fixed.
When SIM cards were switched between WWAN modules there was a misleading warning showing up. This has been fixed.
After configuration of a new WWAN interface it could happen that the new interface was not shown in the list of configured devices until the page was reloaded. This was fixed.

Linux kernel CVEs
CVE-2017-7533 A race condition can lead to local user privilege escalation

SDK example script for SMS receive/transmit failed sometimes
The SDK example script on SMS receive/transmit had an error in the DIO handling. This was fixed. It was improved for better readability and cleaner code as well.

Boot loop after operator error on software update
We have seen devices to run into a boot loop after the administrator performed a configuration update after a partial software update. The bug fix would prevent any configuration updates via file upload until a pending software update was applied on reboot. Nevertheless, it is recommended to reboot the device after performing a software update.

GPS got stuck under certain condition
Sometimes the GPS module (issue was seen at ME909u) got stuck and would not produce a fix until system restart. This was fixed.

Memory leak in SMS send function
When sending via an SSH connection, temporary files were sometimes not deleted if the connection was interrupted too early by the SSH client. If that happened very often, */tmp/* directory could fill up with effect to the operating system. That was fixed.

Do not forward packages of local networks
Packets which belonged to networks of local interfaces were routed over IPsec links even though they were neither originated from, nor targeted to the router (iptables FORWARD chain). That was fixed.

SPL update failed
In very rare occasions it could happen that an update of the SPL boot loader failed. We have seen that on devices which were up for about one year without reboot. To guarantee a proper update, the updater will check the up-time and reject updates if the device has not been rebooted for a long time.

Disabled forwarding of DHCP offers

In setups with more than one WAN link, DHCP offers on one of the WAN links were sometimes forwarded to the other WAN interface. This behavior was not intended and got fixed by disabling forwarding on WAN links until the link is fully operational and all firewall rules apply.

GPS supervision

We have seen situations where the GPS failed to provide data, but the supervision did not trigger a restart of the GPS or of the router. The root cause for the missing GPS data was fixed as well as the behaviour of the GPS supervision in a GPS daemon failure state.

Voice daemon fails and triggers reboot

There have been situations where the voice daemon failed to start and triggered a system reboot. The voice daemon was fixed.

Group alias of nobody to nogroup added

There was a case where a customer relied on the existence of the system group nobody for advanced expert mode OpenVPN configuration. For backwards compatibility with the existing configuration, the group nobody was created as alias to nogroup.

SNMP users not created on configuration update

SNMP users were not created when applying a configuration file. Therefore, SNMP requests with these user credentials failed. This was fixed.

MG102i port Ethernet 5 not turned off

Even when disabled port, Ethernet 5 was not switched off and still showed link activity. The port is now shut down correctly.

SDK improvements

Due to a failure in parameter check, `nm_modbus_reply` could fail even though the given parameters were correct. This was fixed.
In rare conditions `nb_status` returned NULL instead of data even though the request was legit. This was fixed.

Linux Kernel security bug fixes

CVE-2017-16525 Possible attack via crafted USB device in USB serial module
CVE-2017-16531 Possible attack via crafted USB device in kernel USB core
CVE-2017-16534 Possible attack via crafted USB device in kernel USB core
CVE-2017-16535 Possible attack via crafted USB device in kernel USB core
CVE-2017-1000410 Possible remote kernel information leak via Bluetooth L2CAP

VLAN packet loss

If there is an MTU set up on a LAN interface, VLAN packets which are routed over this interface will get lost if the VLAN’s MTU is not set up accordingly. This was fixed.

MTU setup of VLAN interfaces failed

MTU setup was applied to the wrong VLAN interface if there were different VLANs defined on different LAN interfaces. This was fixed.

Security bug fixes

CVE-2018-1000007 curl HTTP authentication leak in redirects
CVE-2017-8816 curl NTLM buffer overflow via integer overflow
CVE-2017-8817 curl FTP wildcard out of bounds read

IPsec expert mode configuration missing in configuration download

The IPsec expert mode files were not included into the configuration files that can be downloaded from the web interface. This was fixed.

Pitfalls / Known Issues

Release 4.0.40.108
2017-11-07

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

Fixes

Protocol server (RS232)
All RS232 functionality options work now – i.e. Protocol server with set of protocols such as Modbus, IEC101, DNP3, etc.

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.

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

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.

Opening several parallel SSH sessions for user admin fails
When several parallel SSH connections for user admin were opened at the same time, no more connections would be established. A failure in CLI console memory management was fixed.

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.

SDK read from bigger temporary files failed
Due to a misaligned buffer offset, reading temporary files bigger than 1024 Bytes failed.

Mount storage from SDK
Fixed an error when trying to mount USB storage from SDK script.

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*).

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.

Do not 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.

Pitfalls

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 which have an inconsistent configuration. Please double check that your IPsec configuration is sane before performing an update.

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.

Known Issues

Release 4.0.40.107
2017-08-01

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

TCP Timestamps
TCP timestamps are part of the PAWS (Protection Against Wrapped Sequence numbers) mechanism which avoid that TCP sequence numbers will wrap and break long data stream transfers on a very fast network connection. However, if TCP timestamps are enabled, a remote attacker can guess the up-time of the system which may indicate that no recent security patches have been applied. If desired, this option can be turned off now.

SCEP CA Identifier
We have added option to configure the CA identifier which is used to pair with the SCEP server.

Number of Firewall Groups/Rules
The number of firewall groups has been increased from 5 to 10. The number of firewall rules has been increased from 35 to 50.

Secondary DHCP Relay Server
It is now possible to specify a secondary DHCP relay server.

GPS Flap Detection
Under some rare circumstances it happened that the GPS signal was flapping and not getting stable anymore. It is now possible to set `surveyor.gnss.maxflaps` (max. number of flaps per 5min) and reset the module if exceeded.

QoS and WLAN EAP
If QoS was operating on a WLAN interface it may have happened that EAP packets were not delivered in time. They will now pass through the scheduler without any restriction.

New Events
Added system-error and system-no-error events which indicate service failures.

Signature Algorithm for Certificates
It is now possible to configure the signature algorithm used when creating certificates.

Improved SMS Management
The SMS daemon is now able to handle scrambled message indexes. Usually this does not happen, but will be covered now.

IP Address of WLAN Clients
The IP address of WLAN clients will be shown in CLI/GUI even if it has not been assigned via DHCP.

Drop ICMP Packets with Timestamps
With ICMP timestamps enabled, a remote attacker might be able to guess the uptime of the system. Thus, any ICMP packets containing timestamps are now being dropped.

Fixes

ME909 Network Registration
Some private networks require the APN to be set prior to attaching to the network which was missing for Huawei ME909 modems. This has been resolved.

IPsec IKE Phase2 Defaults
If the IPsec peer disagreed about IKE phase 2 proposals, it fell back to a set of default algorithms. This behaviour was not intended and was switched off.

SDK-Startup Trigger after Software Update
The sdk-startup trigger didn't work on first bootup after a software update. This has been fixed.

Events via SMS/E-Mail
If the event manager was configured to send both, E-Mail and SMS, it may have failed. That did not happen when using either E-Mail or SMS.

OpenVPN Startup
In some rare cases, the OpenVPN tunnel did not come up because its previous socket has not been closed properly. This has been fixed.

Extended Routes Not Applied
In case of more than one wanlink, with extended routes bound to a lower-prio WAN link, it may have occurred that routes were not set up if the link switched back to the first WAN link. This has been fixed.

SDK Fixes
The `nb_transfer_post` function failed in case of an HTTPS URL. The `nb_ping` function wasn't able to ping a host located in a remote IPsec network and if the WAN link was using Ethernet. The issues have been fixed.

WLAN Antenna Gain
The WLAN antenna gain setting is now applied correctly.

GUI Fixes
Reset button did not reset all debug levels to default values.
Automatic change of DHCP range failed on IP change.
Switch WLAN off if mode is switched back to disabled.
IPsec Tunnel Configuration could not be deleted.
Only offer download button if IPsec clients are enabled.
Add certificates to expert mode files.
Don't switch to certificates page when generating IPsec clients.
Use correct tunnel identifier when creating IPsec client expert mode files.
Fixed downloading of IPsec expert mode files.
The GUI did show the same bitrate for all connected WLAN clients.

Security Fixes
Strongswan IPsec received fixes for the following CVEs: CVE-2017-9022, CVE-2017-9023
The kernel received fixes for the following CVEs: CVE-2017-7308, CVE-2017-7472

Pitfalls

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 which have an inconsistent configuration. Please double check that your IPsec configuration is sane before performing an update.

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.

Known Issues

Protocol Server is not working
If the serial communication is being used in your application, use the 3.8.40.110 firmware instead of the 4.0.40.x. Protocol server is not working in 4.0.40.x firmwares.

Release 4.0.40.106
2017-05-04

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

Power Down on Deactivated USB Ports
Deactivated USB ports will be now without power.

SDK Debug Levels
It is now possible to set, get and reset the debug level of system daemons.

Updating Backup Configuration
The backup configuration, i.e. the configuration stored during a software update, can now be updated by using the CLI with `-b` switch. The corresponding configuration will be applied when the software update is being finished at next reboot.

Fixes

GUI Fixes
The web manager is now throwing a warning in case of unapplied configuration settings. It appeared that the PFS option got lost when reconfiguring IPsec. It also appeared that the OpenVPN connection status was not displayed properly. The DIO page is now refreshing and properly showing the status of digital input ports. Remember WLAN AP settings on channel scan.

Configuration Update with Volatile Entities
Volatile configuration entities are now applied correctly.

USB Adapters via Hub
Serial or Ethernet USB adapters were not properly detected if connected via an additional USB hub. This has been fixed.

SNMP Access to USM User Table
Remote SNMP write access to usmUser table is now forbidden.

Multicast over GRE
It appeared that multicast packets were not forwarded over a GRE tunnel. This has been fixed.

IPsec Traffic for Alias Address
If IPsec was used with a default gateway, it appeared that local traffic for an alias address was sent towards the tunnel. This has been fixed.

Extended Routes / Discard If Down
The "discard if down" option, which shall drop matching packets if the corresponding interface is down, was not applied in some cases. This has been fixed.

SDK Fixes
The `nb_restart` function did not properly check the given service name. The `nb_email_send` function did not properly check the given email address and threw an incorrect return code in some cases. Uploading SSH keys via the `nb_update_sshkeys` function failed sometimes. The `nb_voice` functions did not successfully establish a call. The `nb_config_set` did not properly handle quoted config values. The issues have been fixed.

OpenVPN Pushed Client Routes
An OpenVPN server did not push any routes of other clients to a client. This has been fixed.

Firewall Loopback Rules

It appeared that no INPUT rule was created if source and destination was set to LOCAL. This has been fixed.

SSH Server Upgrade

We have upgraded the dropbear SSH server to version 2016.74 and removed support for CBC and MD5 fingerprints.

Security Fixes

It is now possible to disable TCP timestamps. ICMP timestamp messages are now being dropped. The kernel received fixes for the following CVEs:
CVE-2017-6214
CVE-2016-6786
CVE-2017-6001
CVE-2017-5986
CVE-2016-10229
We are not affected by CVE-2017-6074.

Known Issues

IPsec Expert Mode

The IPsec expert mode files are not installed automatically after a software update. Tunnels need to be reconfigured using the GUI/CLI.

No VRRP on Bridged Interfaces

VRRP over bridged interfaces is not implemented.

No SMS Delivery Reports

SMS delivery reports are currently not possible with Option GTM661/GTM671, Huawei EM820 and Sierra MC7710 modems.

No RSTP on Bridged TAP Devices

RSTP does not work on bridged TAP devices.

Device and Protocol Servers are not working

If the serial communication is being used in your application, use the 3.8.40.110 firmware instead of the 4.0.40.x. Device and Protocol servers are not working in 4.0.40.x firmwares.

Release 4.0.40.105
2017-02-22

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

CLI Virtualization Status
The CLI is now able to display status information about any running virtual guests.

Serial Device Server Keepalive
The device server for serial ports supports the keepalive NOP command when using Telnet.

More DHCP Leases
The DHCP server supports more than 100 leases.

SDK Arguments
The arguments for SDK scripts can now contain slashes and colons.

Fixes

Broken WWAN Connection with Huawei MU609
The Huawei MU609 failed to bring up a WWAN connection if a PIN-protected SIM was used. This has been fixed.

Registration Issues ME909
The Huawei ME909 failed to register to LTE with some providers. This has been resolved.

Correct Bitrate
The GUI/CLI reported an incorrect bitrate for WLAN clients. This has been fixed.

Known Issues

IPsec Expert Mode
The IPsec expert mode files are not installed automatically after a software update. Tunnels need to be reconfigured using the GUI/CLI.

No VRRP on Bridged Interfaces
VRRP over bridged interfaces is not implemented.

No SMS Delivery Reports
SMS delivery reports are currently not possible with Option GTM661/GTM671, Huawei EM820 and Sierra MC7710 modems.

No RSTP on Bridged TAP Devices
RSTP does not work on bridged TAP devices.

Device and Protocol Servers are not working
If the serial communication is being used in your application, use the 3.8.40.109 firmware instead of the 4.0.40.104. Device and Protocol servers are not working in 4.0.40.104.

Release 4.0.40.104
2017-02-13

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

New SDK Functions

USSD requests can now be issued using the `nb_ussd_query` function. We further added an uptime function which returns the number of seconds since bootup.

DHCP Server on Alias Address

The DHCP server was restricted to operate on the primary address. It can use the alias address now.

New SNMP Extensions

The `nbGnssTable` is now showing horizontal speed, vertical speed and the track angle. The `nbAdminTable` is now showing the current system date. Counters for downloaded/uploaded data in the `nbWanTable` are now wrapped correctly. The IF-MIB is now returning proper `ifOperStatus` values. We also fixed some typos in the VENDOR MIB description.

TAB Completion for parrotlog

The parrotlog application now expands any parameter if the TAB key is hit.

Enhanced IPsec Supervision

IPsec tunnels will now be reloaded individually if they are down for 1 minute. The whole IPsec service will be restarted if all tunnels are down for 3 minutes.

Fixes

Voice Daemon Failures

Under some circumstances it may happened that the voice daemon terminated if a SIM switch has run at the same time which resulted in a reboot of the system. This has been fixed.

WTP Encrypted WLAN

Managed WLAN faced a race condition in case of re-keying errors which dropped the associated station. This has been fixed.

EM770 Modem Resets

It happened that a Huawei EM770 was not properly recognized after a reset. This has been fixed.

WWAN Connections Not Dialed

It occurred in very rare cases that the WWAN connection could not be dialed. This has been fixed.

Catch Broken GPS Coordinates

The GPS daemon can now detect out-of-bounds coordinates and ignore the corresponding NMEA frames. This can be enabled by setting `gpsd.0.maxdist` to a maximum distance. Any frames reporting a bigger linear distance will then be ignored and the module will be reset if the situation does not improve.

No GPS Client Connections

The GPS daemon did not accept new client connections if certain NMEA frames have been retrieved. This issue has been fixed.

IPsec Firewall Issues

It occurred that firewall rules bound to an IPsec interface were not working correctly. Now, expected rules for IPsec peers are only created if IPsec is active.

IPsec Connections with AH SHA512

IPsec connections using the authentication algorithm SHA512 did not come up. This has been fixed.

Static Multicast Routing

It occurred that static multicast routes have not been applied in every case. This has been fixed.

FPGA Ping Check

The FPGA supervision occasionally returned false positives. This has been fixed.

Importing Certificates

Stacked CA certificates or WLAN client keys were not imported correctly. This has been fixed.

SDK Issues

Generating a techsupport via SDK cloud blocks the system.
The `sysinfo` function suffered a memory leak.
The `nb_scan_networks` function accepts uppercase interfaces now.
The `nb_serial_write` function returned zero instead of the number of bytes written.
The `nb_transfer` may have returned an invalid result for https/ftps URLs.

Special Characters in WLAN PSK

Special characters (& and \) have not been applied correctly which made the WLAN client authentication fail. This has been fixed.

DNS Server Configuration

It occurred that the DNS server did not come up if no DHCP server has been configured. This has been fixed.

Empty Configuration After Update

An empty configuration may have been generated if config conversion potentially failed after an update. This has been fixed.

Broken PPPoE Connections

In some cases PPPoE connections did not come up. This has been fixed.

Registration Issues ME909

The Huawei ME909 failed to register to LTE with some providers. This has been resolved.

PUK Unlocking

PUK unlocking failed in certain cases. This has been fixed.

Empty SMS Gateway

Some SIMs do not store the SMS gateway which made the WWAN connection fail. This has been fixed.

QoS ToS/DSCP

The QoS feature neglected the ToS/DSCP bits for some packets. This has been fixed.

Long Bootup

The routers faced long bootups if the serial port was not used for the console. This has been fixed.

GUI Fixes

A software update over the GUI could have failed under some circumstances.
Hidden WLAN SSIDs will not be shown anymore.
The IP-passthrough page is now listing valid interfaces only.
The max. storage size for SDK is now proposing a proper value and unit.
Certificates could only be deleted if all files have been installed.
Particular AT and USSDs queries failed.
The NAPT netmask is now validated correctly. It will be set to /32 if omitted.
Showing network address instead of IP in NAPT rule summary.
The GNSS position page doesn’t block anymore if OpenStreetMap service is not reachable.

The GNSS position page is now able to handle additional charsets.
Several typos on the GNSS and IPsec page have been fixed.
The GUI is now able to show stacked certificates.
Downloading OpenVPN expert mode files has been fixed.

CLI Fixes

The CLI now also shows the netmask of any LAN interfaces.
Scanning the mobile networks timed out in some cases.

Security Fixes

Access to secret configuration variables for non-admin users is now forbidden.
Run factory reset if recovery procedure is triggered via UBOOT.
Don’t trigger unwanted software updates.
The `ntpdate` application has been upgraded to version 4.2.8p9.
The `strongswan` suite has been upgraded to version 5.5.1.
The kernel also received fixes for the following CVEs:
CVE-2016-7910
CVE-2016-7911
CVE-2016-7914
CVE-2016-7915
CVE-2016-7916
CVE-2016-7917
CVE-2016-8646
CVE-2016-8650
CVE-2016-8655
CVE-2016-8666
CVE-2016-9555
CVE-2016-9793
CVE-2016-9794
CVE-2016-9806
We are not affected by CVE-2016-9685 and CVE-2016-10147.

Known Issues

IPsec Expert Mode

The IPsec expert mode files are not installed automatically after a software update. Tunnels need to be reconfigured using the GUI/CLI.

No VRRP on Bridged Interfaces

VRRP over bridged interfaces is not implemented.

No SMS Delivery Reports

SMS delivery reports are currently not possible with Option GTM661/GTM671, Huawei EM820 and Sierra MC7710 modems.

No RSTP on Bridged TAP Devices

RSTP does not work on bridged TAP devices.

Device and Protocol Servers are not working

If the serial communication is being used in your application, use the 3.8.40.109 firmware instead of the 4.0.40.104. Device and Protocol servers are not working in 4.0.40.104.

Release 4.0.40.103
2016-11-07

IMPORTANT: **Firmwares since 3.6.41.x are fully compatible**. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

Firewall Rules for OSPF
It is now possible to filter out OSPF packets by means of firewall rules.

Static Multicast Routing
We have added support for static multicast routes. Apart from IGMP Proxy, they can be used to implement bidirectional multicast routing.

Console on Serial Port
The serial console can now be turned off completely. The KPL/KBOOT images are not required anymore.

SDK Transfers
The `nb_transfer` functions are now supporting ftps, https, imaps, pop3s, smtps and sftp. Files can now be downloaded to /tmp directory. We further fixed a flaw when checking URLs.

New SNMP Extensions
We have added the following SNMP extensions:

- `nbGnssTable:gnssNumSatUsed`
- `nbAdmin::systemError`
- `nbWanTable::wanDataDownloadedRoaming`
- `nbWanTable::wanDataUploadedRoaming`
- `nbWanTable::wanLinkNetmask`
- `nbWwanTable::wwanIccid`
- `nbWlanTable::wlanSignalStrength`
- `nbWlanStationTable`

Further, we have added tables of IF-MIB and IP-MIB.

Support for Disabling Ethernet Ports
It is now possible to turn off dedicated ports of the Ethernet Switch.

Extended Storage
It is now possible to store `syslog` messages and SDK files on extended storage if available.

Additional DH Groups for IPsec
We have added Diffie-Hellman groups 16-21 used for IPsec.

Advanced Hardware Failure Detection
We are now detecting hardware failures at a very early stage and also periodically during runtime.

New Managed WLAN Implementation
We have upgraded to FreeWTP for managing WLAN access-points remotely.

Bootloader Password
The bootloader is now supporting SHA256 salted passwords. The password can now differ from the admin password.

Fixes

Bridged GRE TAP Tunnel
A GRE TAP tunnel bridged to a LAN interface didn't come up.

OpenVPN Tunnel
In some rare cases it happened that the OpenVPN client did not come up. This has been fixed. The OpenVPN status page is now properly displaying connected clients.

Invalid WWAN RSSI Value
The RSSI value was not correctly calculated. This has been fixed. We also updated the ASU tables in the Web Manager. The WWAN status page is now showing extended signal information.

SNMP Logging
In some scenarios it might have appeared that SNMP logs exhausted the log filesystem. This has been fixed.

SMS Fixes
Depending on the configuration, it turned out that SMS routes have not been applied correctly. The number of total send/received messages was wrong.

SFTP Transfers
The SFTP client is now creating directories and files with proper permissions.

Preferred Service Type
Depending on your modem, it may have appeared that the configured service type was not met. This has been fixed.

Flapping WLAN Links
The minimum required signal strength of WLAN client connections was only checked after the link came up which may have led to flapping links. This has been fixed. It's further possible now to configure higher suspend thresholds.

WLAN Configuration
The system faced various issues when setting up WLAN. This has been fixed.

WPA-PSK Passphrase Characters
We now support all characters for the passphrase as defined in IEEE 802.11i-2004.

Auto Update
The URL used for automatic updates now supports further characters like underscores. It is now mandatory to specify a proper config version and admin password when uploading a new configuration.

CLI Fixes
Expanding configuration parameters did not work. This has been fixed.

NAPT ARP Issue
In case NAPT rules were bound to an external Ethernet link it happened that bogus ARP messages have been sent. This has been fixed.

Security Fixes
The kernel has received patches for CVE-2016-7117 and CVE-2016-5195.
Serial interface – Device and Protocol server, Modbus TCP
It was not possible to configure the Device server correctly due to "Idle timeout" check. This is fixed. Improvements to Protocol server and Modbus TCP functionality have been applied.

Known Issues

No VRRP on Bridged Interfaces
VRRP over bridged interfaces is not implemented.

No SMS Delivery Reports

SMS delivery reports are currently not possible with Option GTM661/GTM671, Huawei EM820 and Sierra MC7710 modems.

No RSTP on Bridged TAP Devices

RSTP does not work on bridged TAP devices.

Device and Protocol Servers are not working

If the serial communication is being used in your application, use the 3.8.40.108 firmware instead of the 4.0.40.103. Device and Protocol servers are not working in 4.0.40.103.

Pitfalls

CLI/SDK WWAN Signal Status

Please note that the WWAN signal status is now showing RSSI, RSRQ, SINR, RSCP, ECIO as well as level and quality values. The MOBILEx_SIGNAL variable (showing the RSSI value) is now deprecated, but has been retained to be backward-compatible with any scripts.

Serial Port and Console

Starting from the firmware 4.0.40.103, it is no longer required to install dedicated SPL/UBOOT images to avoid printouts on the external serial port. The SPL init string SPL Vx.x.x.x has been removed, please adapt any scripts which rely on that.

Release 4.0.40.102
2016-09-19

IMPORTANT: Firmwares since 3.6.41.x are fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings *(only if you need to use the serial interface Protocol server functionality)*.

New Functionalities

Kernel/System Upgrade
We have migrated to OpenWRT Chaos Calmer which includes an upgrade to Linux Kernel 3.18.16 and recent versions of the packages. This comes with improvements and security fixes for specific packages. The overall routing performance has been increased significantly. Please note that the toolchain has changed from 4.4.5_uClibc-0.9.31 to 4.8-linaro_uClibc-0.9.33.2.

Bridged GRE TAP Interfaces
It is now possible to bridge a GRE TAP tunnel to a LAN interface.

DynDNS TSIG Update
Support for dynamic DNS updates via TSIG has been added. Transaction SIGnature (TSIG) is a secure mechanism to authenticate updates of a zone in the DNS database.

Enhanced Certificate Management
The certificate management has been enhanced. The signature algorithms SHA1, SHA256 and SHA512 and custom Diffie-Hellman primes can now be used when creating certificates. It is further possible to upload authorized keys used for authenticating at the SSH server. Certificate enrollment over SSCEP has been extended and made compatible with Microsoft Windows Server.

Enhanced Firmware Update
A progress bar is now shown when updating the firmware of a module. In addition, the update procedure for the modems ME909 and MU609 has been revised.

New Extensions for Extended Routes
It is now possible to force packets to be forwarded over a specific interface and discard them if the interface is down.

Disable USB Ports
The USB port can be disabled now in order to avoid running any USB code. The USB power supply remains active.

Support for USB Ethernet Asix Adapter
Asix-based USB Ethernet adapters are now supported.

Firewall Logging
Logging of firewall activities can now be achieved by enabling a flag in the firewall rule. This option generates system log entries if a rule has matched.

IKEv2 for IPsec
We have migrated to StrongSwan 5.3.4 and added support for IKEv2 and MOBIKE (RFC 4555). It is also possible to configure Perfect Forward Secrecy (PFS) in detail.
IPsec Expert Mode
IPsec expert mode files can now be generated and uploaded. Currently, this is limited to PKI server mode.

Improved WLAN Roaming
We improved WLAN background scanning to faster detect nearby stations which guarantees seamless handover to access points with higher signal strength.

Managed WLAN over CAPWAP

We have implemented the Control And Provisioning of Wireless Access Points (CAPWAP) protocol according to RFC 5415. With CAPWAP it is possible to control and monitor the WLAN access-point of the router remotely.

Masquerading by Source Address

It is now possible to perform masquerading for specific source addresses.

Multipath TCP

Support for Multipath-TCP (RFC 6824) has been added. MPTCP can be used to establish a TCP connection with multiple paths in order to maximize resource usage and increase redundancy.

Multiple Admin Accounts

Configuring multiple admin users is now possible.

NAPT Enhancements

The target or source address can now be specified for NAPT rules.

OPC-UA SDK Functions

The SDK has been extended with functions to communicate with an OPC-UA server. The OPC Unified Architecture (OPC-UA) protocol suite provides a cross-platform service-oriented architecture and corresponds to an industry standard that enables software to connect devices, machines and systems from different manufacturers using same interface.

OSPF/BGP

The Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) routing protocols have been added.

Multiple OpenVPN Client Networks

It is now possible to specify multiple client networks behind an OpenVPN tunnel.

SDK Extensions

We added support for PCRE (Perl Compatible Regular Expressions) in SDK scripts. It is also possible now to send SNMPv3 trap/inform notifications. Functions for mounting and accessing storage media have been extended. The `recvmsg` function is now able to return the source address of the sender. Using the `nb_userpage_register` function one can now create webpages which are also visible for non-admin users.

Partial Configuration Update

It is now possible to update the system configuration partially, that means only specific parts of the configuration without resetting other values to factory default.

QoS Bandwidth Congestion

QoS has been extended to automatically measure the bandwidth of a link and adapt the queue sizes accordingly.

QoS for OpenVPN

Running QoS on top of OpenVPN connections is now possible.

RSTP

It’s now possible to perform the Rapid Spanning Tree Protocol (RSTP) according to IEEE 802.1D on top of software-bridged Ethernet ports.

SMS Short Number

Support for sending messages to short codes has been added.

New WWAN Features

The required signal strength can be specified by means of link quality levels rather than just the RSSI value. You can further specify the mobile bands to which the modem shall register (if supported).

SNMP Extensions

We have extended the `nbAdminTable` for storing and scheduling software and configuration updates. Please take a look at the VENDOR-MIB for getting further information.

Updates over SFTP
Software and configuration updates over SFTP are now possible.

Virtualization with LXC
We added support for LXC (see linuxcontainers.org) which allows customers to set up an isolated operating system for running any third-party applications.

Additional WLAN Features
We have added support for Protected Management Frames (PMF) according to IEEE 802.11w. It is further possible now to limit the available ciphers and run 802.11n with CCMP only. One may also enable the SGI20/SGI40 option if supported by the WLAN module.

CoovaChilli Hotspot
The CoovaChilli captive portal can be provided over a dedicated software release including support for Walled Gardens, RADIUS accounting and bandwidth limiting.

Configurable IP-Passthrough Network
It is now possible to configure the WAN network which will be passed-through to a LAN host and to communicate with other devices in that network.

SDK Workdays/Weekend Triggers
Triggering scripts only on workdays or weekend is now possible.

WEP Hex Keys for WLAN Client
It is now possible to configure WEP40/WEP104 keys in ASCII and HEX notation.

Fixes

Flipping WAN Links
It was not possible to flip configured WAN links using the Web Manager. This has been fixed.

System Time over GPS
The system has not been notified in case the time has been synchronized over GPS. This has been fixed.

QoS Issues
The QoS page showed no configurable interfaces. The daemon is now also more robust in case of a bogus configuration.

TCP Challenge ACK
The kernel has been patched to make TCP challenge ACKs less predictable (see CVE-2016-5696).

SMS Filtering
It appeared that all messages have been filtered out although a rule existed which should have allowed messages from a particular number. This has been fixed.

Invalid Signal Information on Huawei EM820W
Under some circumstances it appeared that the retrieved RSCP/ECIO value was declared as invalid on Huawei EM820W. This has been fixed.

Force DHCP Static Address for Ethernet Port
The DHCP server has assigned a new address out of the lease pool and not the configured static address if a new device has been attached to the corresponding Ethernet port. This has been fixed.

SNMP Upload
Uploading the configuration or system log via SNMP failed due to a bogus URL check. This has been fixed.

GLONASS on Huawei ME909

Receiving information from GLONASS satellites was not working. This has been fixed. Setting up GLONASS on ME909 raised an error with older firmware versions. This has been resolved.

USSD Queries

USSD queries were not working on all modems. They have been verified for the following modems:

- Option GTM661/GTM671
- Huawei EM820
- Huawei ME909
- Sierra MC7710

OpenVPN Client Management

In case an OpenVPN client network was configured it was not possible to add a server network. This has been fixed.

Fixes for SNMP Extensions

It appeared that `configUpdated`, `softwareUpdated`, `altConfigUpdated` and `altSoftwareUpdated` returned an incorrect date response. Further, the last config activation and installation date was not recorded properly. The software and config profiles will now be updated immediately. It is not anymore required to specify the remote Engine ID for SNMP traps.

Invalid WLAN RSSI Range

In very rare cases the link-manager did not bring up the WLAN connection due to a bogus signal strength calculation. This has been fixed.

QoS Bandwith Configuration

It was not possible to adjust the download bandwidth of a QoS queue if congestion was set to fixed.

SDK Fixes

The `nb_transfer_get` function did not return a failure in case of an invalid authentication error. Further, the `nb_can_setattr` did not correctly set up the listen mode. The issues have been fixed.

Import of CAPWAP Certificates

Importing CA bundle files for CAPWAP failed under some circumstances. This has been fixed.

IP-Passthrough Routing

Routes for IP-Passthrough are now set up correctly.

Known Issues

No VRRP on Bridged Interfaces

VRRP over bridged interfaces is not implemented.

No SMS Delivery Reports

SMS delivery reports are currently not possible with Option GTM661/GTM671, Huawei EM820 and Sierra MC7710 modems.

No RSTP on Bridged TAP Devices

RSTP does not work on bridged TAP devices.