M!DGE Release Notes
Firmware version 4.2.40.xxx

Release 4.2.40.104
2019-05-07

Note: The firmware **4.2.40.104** is the first official firmware available on our website and for mass production from 4.2.40.x firmware family.

IMPORTANT: ECC Conversion
The flash on M!DGE routers provides an automated error correction using ECC. We changed the ECC length from 1-bit ECC to 4-bit ECC which provides better error correction. On the first boot after the software update has been performed, the data on the flash memory are automatically converted to use the new ECC setup. While this conversion is being performed, the LED diodes are “on” for about 30 seconds. If you switch back to an older software release like 4.0.40.x, the migration is reverted.
We tested updates and downgrades to and from 4.0.40.x and 3.8.40.x. Updates to or from older versions are not supported. If you run an older release or want to downgrade to an older release, you are advised to migrate via 4.0.40.x as an intermediate release. To revert the migration on downgrade, the SPL boot loader release 4.1.40.x stays in place. It can be downgraded in a second software 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 4.0.40.x and older for systems running 4.1.40.x and newer. If you want to use recovery images, please contact our support at support@racom.eu.

New Functionalities

SW update package validated before upload
An invalid SW update package is identified in the web interface before the actual transfer to the target was performed skipping the process of slow upload of potential invalid packages via mobile network. The new architecture also allows us to provide better and more detailed feedback on the current update status.

New version of igmpproxy
Igmpproxy was updated to version 0.2.1. This also fixes a bug on interfaces with an alias IP setup.

HTTPS access with client certificates
Functions which communicate with HTTPS-Servers (like SW update from URL or SDK) can now authenticate with client-certificate and key.

MQTT publishing from SDK
Functions for publishing MQTT messages were added to the SDK scripting language.

Password hashes replace encrypted passwords in configuration
We changed our password handling to use cryptographic hashes instead of symmetric encrypted passwords wherever possible. Therefore, you have to provide the administrator password for downgrading to older SW releases as these still rely on the passwords to be stored on the device.
For SNMP access the passwords still need to be available. Therefore. users which shall be able to log in via SNMP need the new setting "Store password in device" to be enabled.

Wait for configuration change task to be finished
Changing a configuration setting via CLI or SDK does not block. A new function was implemented to request if all pending tasks have been finished and it is safe to send new configuration change requests.

uBlox TOBY-L2 support
The uBlox Toby-L2 LTE modem is now supported.

Number of VLANs increased
It is now possible to configure up to 10 VLANs instead of 5.

Update of time zone data
North Korea switched back to +09 on 2018-05-05. Our best wishes to all Korean people.

LED configuration
All LEDs except for "STAT" can be configured to different function like LAN, WAN, WLAN, WWAN, etc.

Bridges without STP
It is possible now to switch off STP completely on bridge-devices.

GUI improvements
Allowing Upload of keys and certificates in nested p12 files.
IP pass-through setup failed on web interface with recent SW releases.
Obsolete GUI interfaces have been removed.

Configuration of NTP server stratum
The stratum of NTP server in case of GNSS sync or time from internal clock can be configured now. As these sources are not very accurate this feature should be used with care. Please contact our customer support for detailed information.

Refactory of config converter
Our config conversion tool `cfconvert` which is responsible for converting older and newer configuration files to the configuration release needed by the current version was refactored speeding up this step of SW update or configuration apply by factor or 3-5 and reducing the required flash space by several hundreds of kB which was required for implementation of other features on older hardware like M!DGE or MG102i with very limited flash space.
As a side effect the conversion to configuration versions other than the one used by the current SW release is not supported any more. In normal operation this is not needed anyway. If you have such a requirement please contact our technical support.

Support for additional IPsec parameters in expert mode configuration
Expert mode files now support additional parameter rightsigkey and allow upload of certificates and keys which are encrypted with a pass phrase in expert mode configuration files.

More status information on SWI interface for QMI based WWAN modules
The WWAN status information was extended to show information on SWI status.

IPsec now supports certificate chains
You can now upload certificate chains for IPsec connection establishment.

U-blox Toby L2 Series
The u-blox Toby-L200 and Toby-L201 are now supported.

Watchdog supervision of OSPF and BGP daemon
OSPF and BGP daemon are now supervised by watchdog. This will result in a reboot and reinitialization of the router if one of these daemons crashes.

APN credentials printed to logs
With debug set to maximum, the login credentials for the WWAN APN were printed to the logs. In most setups there is no secret data in APN credentials as they are common for all customers of one provider and can be looked up on the Internet, but if you use a private APN they should not show up in the logs.

Security Fixes

Update of Lighttpd
Lighttpd was updated to version 1.4.50. On older releases Security relevant issues were back ported.
CVE-2015-3200: Injection of log entries fixed on lighttpd

Log display in web interface vulnerable to Cross-Site-Scripting (XSS) attack
The web interface which displays the system log was vulnerable to JavaScript XSS attacks. An attacker capable of placing malicious content in the system log could execute JavaScript code in the web browser of the user.

Security bug fixes on 3rd party SW packages
CVE-2015-3200: Use-after-free fixed in Linux kernel

Security bug fixes in 3rd party SW packages
CVE-2018-14526 Unauthenticated EAPOL-Key decryption in wpa_supplicant

Security fixes in 3rd party and open source packages
CVE-2018-1000500 Busybox contains a Missing SSL certificate validation vulnerability in wget applet.
CVE-2019-8912 Linux kernel had possible use-after-free in sockfs_setattr.
CVE-2018-0732 OpenSSL client DoS due to large DH parameter
CVE-2018-0737 OpenSSL cache timing vulnerability in RSA Key Generation
CVE-2018-5407 OpenSSL microarchitecture timing vulnerability in ECC scalar multiplication
CVE-2018-0734 OpenSSL timing vulnerability in DSA signature generation
CVE-2019-1559 OpenSSL 0-byte record padding oracle

Fixes

Serial Interface configuration
On M!DGE2 with more than one serial interface, only one could be configured for special purpose like device server or protocol server. The first interface could not be changed to anything else but ‘login console’. This was fixed and now all serial interfaces can be used for any purpose.

LAN as WAN configuration
The WAN configuration of a LAN interface was not applied correctly. This has been fixed.

IP packets with DSCP tag not processed by M!DGE2
Special IP packets with DSCP tag 0x40 did not pass the internal network switch of M!DGE2 and therefore could not be received, sent or forwarded. This has been fixed.

SDK improvements
The SDK function `nb_can_setattr` failed if the optional parameter restart was different from 0.
Fixed typo in modification time of files in `nb_transfer_list`.

Mismatch between VLAN network settings and DHCP settings triggers reboot
In situations where the VLAN network settings (network address/netmask) did not fit with the DHCP range configured for that network, the router would go into reboot. This was fixed. Now the DHCP server on the mis-configured interface will not be started and a warning is given to the user.

Authorities certificates were not used for all HTTPS downloads
Some functions where data are downloaded from a server the "Authorities" certificates were not used. E.g. it was not possible to update WWAN module firmware from HTTPS.

GUI improvements
Changing the priority of WAN interfaces in GUI did change bridged WLAN client interface setup. WAN links are displayed as bridgeable devices. This has been fixed.
Changing between 4G-Only and automatic increased the amount of transferred data. This was a failure of data display and did not affect the actual data traffic.
The interface numbering was wrong during modem firmware update. This has been fixed.
WAN interfaces could be reconfigured to LAN if port assignment was changed in GUI.
Changes on port setup could switch configured WAN interfaces to act as LAN interfaces.
User data from the web administration interface was not escaped correctly in some cases.
Clicking on 'Cancel' in the certificate settings accidentally applied the changes.

Certification installation over CLI
It was not possible to install WLAN certifications for client mode over the CLI command. That has been fixed.

SNMP walk timeout
In certain cases, an SNMP timeout could occur during an SNMP walk. That has been fixed.

uBlox TOBY-L2 improvements
Clients connected to the LAN side of the router could not communicate to the WAN network, because IP forwarding was disabled. That has been fixed.

SNMP: unknown type in vendor MIB
The MGTrapHistoryEntry SNMP MIB was not standard conform. That has been fixed.

Fixed SDK example script
The SDK example script 'dio-server.are' contained a logical error that could trigger an error on runtime.

Soft bridges sometimes not in UP state after configuration
Depending on which devices were bridged on one of the soft bridges (BR1, BR2), the soft bridge was not set to state UP if no local IP address was configured. Therefore, packet forwarding between these devices failed.

SW update URL was identified as invalid by mistake
Due to internal escape sequence URLs containing special characters like '&' were identified as invalid.

Usernames starting with 'admin' or 'root' not able to login
Additional users starting with 'admin' or 'root' like 'admin-user' were not able to login after change of administrator password.

Ping supervision failed on IP pass-through
In IP pass-through the ping supervision failed to contact the server and therefore restarted the router even if the WWAN connection was fine.
Certificate key handling
Changing the certificate key of the system could fail and leave the system without usable certificate keys. This was fixed.

Empty user password affected other users
If the setting 'user.0.password' contained an empty string, all other users were not able to log in any more. This is not a valid configuration anyway, but it was not intended behaviour neither and therefore was fixed.

Optimized start sequence for WWAN modules
In rare situations the system start might fail due to high current consumption of WWAN on upstart. This was fixed by optimized start-up sequence.

Make sure WWAN module is attached to network on dial
In the test lab, we have seen some WWAN modules failing to auto-attach to network under test conditions. If that happens, we now send an explicit attach command. We are not aware of this happening in a real-world environment, but if it should happen it should speed up reconnect in detached state for the affected modules.

Improvements of OSPF daemon
Under very heavy load the OSPF daemon could crash. These situations have been covered and packets which cannot be handled will be dropped instead. The daemon is also under watchdog supervision now.

Missing routing entry for OpenVPN server
Under certain conditions, the setup system failed to add a mandatory route entry for the OpenVPN server. This was fixed.

GUI improvements
When changing the network IP and mask of a bridge device, the DHCP settings were not checked. Now the GUI will propose appropriate new settings for the DHCP server.
The deletion of VLAN interfaces could lead to DHCP configuration failures. This has been fixed.
The web interface did not show the same signal quality information that was displayed by LED colour. This was fixed. Both interfaces use the same data source now.
An inconsistency in menu of the web interface was fixed.
Setup of a LAN port as WAN with Static IP gave a misleading warning on invalid DHCP setup.
Time-based SDK trigger setup was simplified.

LAN as WAN configuration
The WAN configuration of a LAN interface was not applied correctly. This has been fixed.

Several WWAN links on the same WWAN module
A setup with different WWAN links on the same WWAN module with the same SIM card and different APN failed to establish a connection. This was fixed. Several links sharing common recourses like WWAN module or SIM card can be configured as switchover.

No WWAN connection due to invalid SMS centre
On a network in Dubai we saw the WWAN connection failed with an error message due to invalid SMS centre message from the provider. This is handled now and will only produce a warning in the logs. To use SMS feature in such an environment, the SMS centre configuration has to be set up manually.

Ethernet switch framework not aware of virtual port mapping
In situations where the logical port assignment does not match the physical port assignment and some ports are turned off, the Ethernet switch framework put down wrong ports periodically. This was fixed.

Setting or getting DIO state with SNMP failed
A new DIO interface introduced in 4.2.0 failed on SNMP. That was fixed.

Toby-L2 preferred service
No WWAN connection was possible anymore if the preferred service was changed. This has been fixed.

Toby-L2
The WWAN connection did not reconnect after a signal loss has occurred if 4G only was configured. This has been fixed.

WWAN module sometimes failed to reconnect
Under certain conditions we have seen ME909u and ME909s modules to take very long time to reconnect. This was a result of missing state check before module reset and fixed by enhanced bring-up procedure.

SNMP engineID
The SNMP engineID was not generated correctly. The engineID is now generated by using the Serial number of the device.

USB Tethering
No IP configuration for USB tethering devices were possible. This has been fixed.

Known Issues