M!DGE2 - Release Notes

Release 4.6.40.105

2023-11-06

- **New Functionalities:**
  - **Support for ECC Certificates and Keys** - Importing Elliptic curve cryptography certificates and keys is now supported.
  - **Update of 3rd party open-source packages** - The tcpdump debug tool was updated to version 4.9.3.
  - **Update of libidn2** - System library libidn2 was updated to version 2.3.2.
  - **SSL certificate generation** - Using random serial numbers for generated SSL certificates.
  - **IPsec improvements** - Local and remote IKE ports are now configurable.
  - **Scheduled WWAN module restart** - Some customers faced problems with stationary devices which did sporadically disconnect from the base station. A nightly reset feature was introduced. You can configure it within the Interfaces – Mobile menu.
  - **IPsec** - A configurable dead peer detection for IKEv2 based tunnels has been added.
- **Security Fixes:**
  - **Security issues in Mosquitto MQTT library**
    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.
    CVE-2021-34432: The server will crash if the client tries to send a PUBLISH packet with topic length=0.
    CVE-2021-41039: An MQTT v5 client connecting with a large number of user properties could cause excessive CPU usage, leading to a loss of performance and possible denial of service.
  - **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.
  - **Security issues in the D-Bus**
    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.
  - **Security patches for strongSwan IPsec**
    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.
    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 EAPSuccess 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.
  - **Security patches for libpcre**
    CVE-2020-14155: An integer overflow via a large number after a special substring may occur.
  - **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.

- **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.
- **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.
- **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.
- **Security patches for Dropbear SSH**
  CVE-2020-36254: The scp tool in Dropbear before 2020.79 mishandled the filename of . or an empty filename.
- **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 M!DGE2 SW, 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 M!DGE2 SW deferred authentication is not used and might only be configured via users expert mode file configuration.
- **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 M!DGE2 SW anyway.
  CVE-2020-15861: Due to incorrect handling of symlinks, sensitive data could be disclosed.
- **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.
- **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.

- **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 M!DGE2 SW, 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 M!DGE2 SW, only authenticated administrative users are able to upload files.
- **Security patches for libssh2 system library**
  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.
- **Security patches for libyang used by FRRouting**
  CVE-2021-28902: Possible NULL pointer dereference could lead to program crash and denial of service.
  CVE-2021-28906: Possible NULL pointer dereference could lead to program crash and denial of service.
  CVE-2021-28903: Possible denial of service by uncaught infinite recursion.
  CVE-2021-28904: Possible NULL pointer dereference could lead to program crash and denial of service.
  CVE-2021-28905: Possible DoS by malformed assert on eventually NULL object.
- **Security issues fixed in U-Boot**
  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.
  CVE-2022-30552: buffer overflow
- **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.
- **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. Security issues in the PHP scripting language.
- **Security issues in GnuTLS library used by radius client**
  CVE-2020-11501: GnuTLS uses incorrect cryptography for DTLS. The DTLS client always uses 32zero bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol. 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.
  CVE-2021-20231: A potential use after free may lead to memory corruption.
  CVE-2021-20232: A potential use after free may lead to memory corruption.

- **Fixes:**
  - **GUI improvements**
    The tabbing links under System - Settings were broken. This was fixed.
    If a 3rd party software package was published under more than one license, the link to the second license text was broken. This was fixed.
    The web interface WAN status page did not show IPv6 address. This was fixed.
    Links to support web sites for trouble shooting were updated.

- **SNMP v1 broken**
  With previous 4.6 software versions, the SNMP server did not answer on SNMP v1 requests any more. This was fixed.
- **OpenVPN generated invalid client configuration files**
  The client configuration files generated by M!DGE2 SW contained an invalid protocol entry making it impossible to use them for proper client configuration. This was fixed. You may have to regenerate client configuration files if you faced this problem.
- **DHCP requests failed if 802.1X authenticator was enabled**
  In some setups the DHCP server did not answer on DHCP requests on ports where the 802.1X authenticator was enabled. This was fixed.
- **STP malfunction**
  STP was not enabled if configured. This was fixed.
- **GUI improvements**
  The WWAN provider selection list was missing IPv6 APNs. This was fixed.
  If too many WAN interfaces were added a generic error message was shown. This was replaced by a more specific and more helpful message.
  VLAN based WAN interfaces configuration was not properly propagated to the configurations in previous 4.6 SW versions. This was fixed.
  Configuration from older releases were displayed incorrectly, but worked as expected.
  A VLAN WAN link remained in the list of WAN links when the underlying VLAN interface was removed.
  The configuration file download failed in certain cases. This issue was fixed.
  In previous 4.6 SW versions, the underscore symbol was rejected in the username and password fields for the automatic configuration update mechanism. This issue was fixed.
  On certain pages, the footer elements were displayed incorrectly, this issue was fixed.
  The system log display is no longer jumping to the first line each time a new message arrives.
  After changing the LAN IP address range, the DHCP server range notification pop-up was not displayed.
  When configuring a new IP address of the interface that is currently used for reaching the web interface, the browser will be redirected to the newly configured address.
- **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 the SIM's PUK2 needed or permanently locked. This was found in internal review and fixed.
- **Firewall rules applied incorrectly**
  Forwarding firewall rules for IPv4 were applied twice in the INPUT direction, instead of once INPUT and once OUTPUT direction. This was fixed.
- **IPsec improvements**
  Depending on the configuration, the expert mode files generated on the server for clients had an invalid syntax. This was fixed.
- **OpenVPN AUTH FAILED could lead to reboot**
  In certain cases, failed OpenVPN authentication led to a reboot. This was fixed.
- **SDK improvements**
  Outgoing voice calls could not be started from SDK scripts. This was fixed.
- **LTE requires 2nd antenna**
  It was possible to select the number of antennas in the LTE setup. Nevertheless, the LTE standard makes the 2nd antenna mandatory for background-scans. This feature was discontinued.
- **USB-to-serial adapters not working**
  Some USB-to-serial adapters did not work in older 4.6 software versions because the required kernel module was not probed correctly. This was fixed.

- **WWAN connections without DNS provider failed to connect**
  It was mandatory that a DNS provider is pushed by the network. This is not guaranteed in some private APN networks; depending on the modem type, the connection failed in such cases. The old behavior was restored.
- **Broken OpenVPN after update**
  Some existing OpenVPN configurations in the field could break during the software update process. This was fixed.
- **Watchdog fixes**
  Watchdog had a memory leak in previous 4.6 SW versions. This is fixed.
- **CLI status did not show bridged IPs**
  Client IPs of bridged interfaces were not displayed properly in some cases.
- **SDK fixes**
  The Arena SDK function json_encode now behaves according to the JSON standard.
- **Network fixes**
  Switching link prioritization was deficient in older 4.4 SW versions. This is fixed.
- **DHCP improvements**
  DHCP can now be configured for BR interfaces.
- **WWAN connections**
  The network registration process of modems from the Ublox TOBY-L2 series has been improved.
- **LLDP**
  The LLDP daemon (lldpd) was only started on every second attempt when changing protocols for a currently active lldpd. This issue has been fixed.
- **Configuration upload**
  The upload of larger configurations could result in the router running in a timeout and as a consequence ending up in an error state. This issue has been fixed.
- **Modem fixes**
  TOBY-L2 modems were not reset properly, this issue has been fixed.
- **Serial Console**
  A misconfiguration of the serial console caused output on the serial port when it was disabled, this has been fixed.
- **IPsec improvements**
  Shared networks were not routed correctly when trying to access them directly from the tunnel endpoint and thus were not reachable. This issue has been fixed.
  In IPsec tunnel configurations using "0.0.0.0" or an empty field for a local ID or peer ID of type "IP Address", the tunnel was not established. This issue has been fixed.
- **L2TPv3**
  In previous versions, a bug in the L2TPv3 implementation prevented tunnels with UDP encapsulation to become up. This issue has been fixed.
- **OpenVPN**
  In certain edge conditions, the modification of OpenVPN tunnel settings could hang for a long time and all successive OpenVPN modifications would hang as well until the device was rebooted. This issue was fixed.
- **Webserver configuration**
  Fixed a redirect issue when upgrading to a secure connection. There was no direct security implication.
- **Firewall/IPsec**
  Access to local services on the router itself is no longer disabled for setups with an active IPsec connection configured to use IPsec networks with NAT.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Auto refreshing some pages** — Once the change is applied, the process is started correctly. Settings are also saved successfully, but the process does not finish automatically. Refresh the page manually in such a case (e.g., changing LAN IP address).
  - **WAN setup using "Continue" button** — Do not use the "Continue" button while creating a new WAN interface on any of M!DGE2's ETH port. This might lead to a state in which the WAN is created twice. If this happens, either change the WAN settings back to LAN and repeat the steps without using the "Continue" button, or use the CLI set commands to delete the wrongly created WAN interface (keep the original one, delete the 2nd one).
  - **GRE local IP address configuration lost after software downgrade to 4.4.40.x** — In most of situations, M!DGE2 supports both software upgrades and downgrades and is able to handle correctly the configuration compatibility. If you configured the GRE tunnels with specific source IP addresses and you do the downgrade from 4.6.40.x software back to 4.4.40.x, this parameter is lost. In general, downgrades are not recommended.

Release 4.6.40.103

2023-04-11

Important

Upgrade M!DGE2 software to the latest 4.4.40.115 or 4.6.40.103 release together with Toby module firmware upgrade to the 17.00,A01.02 release. These upgrades mitigate an issue in which the Toby/WWAN module could get "missing" and was no longer possible to utilize cellular connection

- **New Functionalities:**
  - **Firewall features** — Unencrypted outgoing traffic is now actively rejected during IPsec tunnel downtimes.
  - **Firewall improvements** — Explicitly allow outgoing ICMP traffic, that would otherwise be denied/rejected during IPsec tunnels' downtimes due to improved firewall security.
- **Fixes:**
  - **BGP changes** — Link detection is now disabled by default, i.e., routing propagation works even if LAN links are down.
  - **OpenVPN changes** — Cryptographically weak ciphers are now accepted by default on OpenVPN connections for backwards compatibility with legacy OpenVPN setups. For improved security, support for weak ciphers can be disabled. Client configurations exported with weak ciphers enabled cannot be imported into software versions 4.4 and older. This is intended in order to maintain compatibility with current software versions.
  - **IPsec '%any4', left/leftid parameters** — 4.6.40.102 software automatically filled the IPsec 'left' parameter by Left ID value in case the type was "IP". Correct behaviour is to fill '%any4' value. This has been fixed.

- **Automatic DHCP changes** — DHCP range is now automatically changed after LAN IP changes.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Discovery services** — Automatic discovery services (LLDP, CDP, …) do not operate correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.
  - **Auto refreshing some pages** — Once the change is applied, the process is started correctly. Settings are also saved successfully, but the process does not finish automatically. Refresh the page manually in such a case (e.g., changing LAN IP address).
  - **WAN setup using "Continue" button** — Do not use the "Continue" button while creating a new WAN interface on any of M!DGE2's ETH port. This might lead to a state in which the WAN is created twice. If this happens, either change the WAN settings back to LAN and repeat the steps without using the "Continue" button, or use the CLI set commands to delete the wrongly created WAN interface (keep the original one, delete the 2nd one).
  - **GRE local IP address configuration lost after software downgrade to 4.4.40.x** — In most of situations, M!DGE2 supports both software upgrades and downgrades and is able to handle correctly the configuration compatibility. If you configured the GRE tunnels with specific source IP addresses and you do the downgrade from 4.6.40.x software back to 4.4.40.x, this parameter is lost. In general, downgrades are not recommended.

Release 4.6.40.102

2022-06-29

- **New Functionalities:**
  - **GRE source (local) IP** — It is possible to configure source (local) IP for GRE tunnels – this can be important in case of multiple WAN interfaces.
  - **Firewall address translation based on SRC and DST ports** — It is now possible to filter packets for inbound and outbound address translation by source and destination port. So far it was only possible to use either source or destination port.
  - **Increase maximum number of firewall groups** — It is now possible to configure up to 50 firewall groups.
  - **Seamless re-keying on IPsec IKEv2** - IKEv2 requires periodic re-keying. The new option "make-before-break" allows to initiate the re-keying while the connection is still up before the keys expire preventing additional connection down time.
  - **802.1x over Ethernet** — The routers can now be used in a network with 802.1x infrastructure.
  - **STP configuration** — The global STP setup can now be overwritten for individual LAN interfaces.
  - **IPv6 Support** — WAN interfaces and services which connect via WAN do support IPv6 now.
  - **Increase number of Ethernet WAN links** — The maximum number for LAN or VLAN based WAN interfaces was increased to 10.
  - **3rd party open-source packages updated**— mac80211 updated to version v5.10.16-1
    ath10k-ct updated to version 22
    The Linux Kernel was updated to version 4.19.163.
    The udev package was updated to version 3.2.9.

The OpenSSL library was updated to version 1.1.1l.
Quagga was replaced by the actively maintained FRRouting fork in version 7.5.1.
LXC was updated to version 3.1.

- **SDK improvements** — Scanning for mobile networks disabled all WWAN connections. This was changed: Only connections on the WWAN module selected for the scan are dropped, while connections on other WWAN modules are not affected by the scan.
  Additional data is included in Techsupport files to improve maintainability and customer support. This includes logs of start and termination of all SDK jobs, information on jobs which were active at the moment when the Techsupport file was generated and optionally the scripts installed to the system.
  Support for full featured MQTTv5 client.
  M!DGE2 can now be set to a low power sleep mode from SDK with RTC wakeup.
  nb_transfer functions have a new optional parameter for additional HTTP headers and custom FTP commands.
- **PHP-CLI accessible for all users** — It is now possible to enable PHP-CLI for any user. Depending on the general access rights the user may read status information or write configuration settings.
- **Support for Let's Encrypt certificate API** — It is now possible to obtain and renew certificates from Let's Encrypt automatically.
- **CLI improvements** — The command line interface shows active DHCP leases in status output.
- **PLMN change without global WWAN restart** — Changing the allowed PLMN on one WWAN module triggered a restart of all WWAN connections on all modules. This was changed. An ongoing WWAN connection is not interrupted by PLMN change on another connection.
- **Random certificate key** — On initial login from factory state, a random key is generated to store generated and uploaded key encrypted internally. In the past, a dedicated key had to be configured. This is still possible.
- **Number of static multicast routes increased** — It is now possible to configure up to 10 static multicast routes.
- **Reset of WAN-Link statistics via SNMP** — It is now possible to reset the WAN-Link statistics (RX/TX bytes, etc.) via SNMP.
- **STP and RSTP for soft-bridges** — All BR1-BR5 bridges support STP and RSTP settings.
- **More VXLAN tunnels** — The maximum number of VXLAN tunnels was increased from 4 to 10.
- **NTP server answers signed requests with crypto-NAK** — Requests with authentication requests are now answered with crypto-NAK messages according to RFC 5905.
- **SNMP MIB updated** — Some obsolete entries were marked as obsolete and some minor changes were made for better interoperability.
- **Event trigger via PHP-CLI** — It is now possible to trigger a system event via PHP-CLI.
- **GUI improvements** — The configuration interface of multicast routing required to set up a source address. This address was technically not mandatory. It is now possible to configure multicast routing without this address.
  The WWAN configuration via list of known APNs allows to select IP version for the connection.
  The browser's tab display is improved.
  The DNS status was shown in the DNS configuration interface. To be compliant with our general approach, the DNS status information was moved to a dedicated status page.
  Password input was reworked in the web interface. It is now possible to show passwords in clear text for verification.
  It is possible now to run *tcpdump* on all interfaces at the same time. This is helpful in situations where you try to debug a misconfiguration in your routing setup where you don't know on which interface traffic is routed.
  Maximum rate of SMS-send events now configurable.
  The GUI now shows better information on the store password option.
  It is possible to download and upload encrypted configuration files.

- **Security Fixes:**
  - **Security bug-fixes in curl**
    Fixed CVE-2021-22946: Protocol downgrade required TLS bypassed
    Fixed CVE-2021-22924: Bad connection reuse due to flawed path name checks
    Fixed CVE-2021-22947: STARTTLS protocol injection via MITM
    Fixed CVE-2021-22890: TLS 1.3 session ticket proxy host mixup
    Fixed CVE-2020-8169: Partial password leak over DNS on HTTP redirect
  - **Authenticated Remote Code Execution and Privilege Escalation in PHP-CLI** — A user with access to PHP-CLI could inject shell code which was executed with administrative rights. The validation and escaping of command arguments was improved to prevent such an attack. Also, Administrative users were able to inject shell code. But given that they could control the device via PHP-CLI anyway this is not a security issue but considered undesired behavior. This was fixed as well. PHP-CLI is disabled by default as well as the access to PHP-CLI for non-administrative users. If you did not enable them, you are not affected.
  - **Additional HTTP Security Header added to web interface** — The HTTP Content-Security-Policy response header whitelists resources the user agent is allowed to load for a given page. This helps to guard against cross-site scripting attacks (XSS).
  - **Linux kernel security patches** — CVE-2022-0492 fixes missing capabilities check for cgroups.
  - **Security issues fixed in BusyBox package**
    CVE-2018-20679 and CVE-2019-5747: An out of bounds read in udhcp server, client and relay may allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message.
    CVE-2018-1000500 and CVE-2021-42374 - CVE-2021-42386: These CVEs have been fixed in the source code even though they did not apply to the software or were only exploitable by users with administrative status which have full access to the device anyway.
  - **OpenSSL security patches**
    CVE-2021-4160: Actually, M!DGE2 was not affected because this applies to MIPS hardware only. Nevertheless, we applied the patch in case we ever adopt our system to this hardware. For existing M!DGE2 running on ARM or PPC this should have no impact at all.
    CVE-2022-0778 fixed possible remote denial of service attack when parsing certificates. In M!DGE2 only users with administrative rights may install certificates. Therefore, the severity is considered low.
    CVE-2021-3711 Buffer overflow. The relevant bug-fixes for this issue were back-ported.
    CVE-2021-3449: Possible NULL pointer dereferences. A maliciously crafted renegotiation message can provoke a NULL pointer dereference in an SSL server application. The upstream OpenSSL patch was backported.
  - **CVE-2018-25032 zlib denial of service** — The compression library zlib was vulnerable to a memory corruption when compressing input with distant matches. The upstream patches were back-ported to the software.
  - **CVE-2020-12351 BleedingTooth bug in Linux kernel** — Potential security vulnerabilities in BlueZ may allow escalation of privilege or information disclosure.
  - **Update of 3rd party open-source software** — Dnsmasq was updated to release 2.84. This fixed several security vulnerabilities. As long as you sticked with the configuration management framework, M!DGE2 software was not affected by these vulnerabilities due to compilation options and configuration settings which are required to exploit them: CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687.
  - **Authenticated read and delete of arbitrary files via web interface** — A directory traversal mistake made it possible for logged-in administrative users to read and delete arbitrary files on the file system.
  - **Users with CLI shell access could extend their privileges** — For users with CLI shell access, it was possible to open a regular Linux command line shell.

  - **Information breach for user logged in to shell** — A user with limited rights who was logged in to a shell (for example via SSH, Telnet or serial interface) was able to request confidential configuration values. Non-Administrative users are not able to log in into a shell and therefore this attack should not be exploitable, nevertheless the access rights to the configuration management were fixed
  - **Incorrect permission assignment for critical resources** — Some files like /etc/shadow were readable by non-administrator users. This is a potential security risk. It is not possible to configure a login with shell access or read the file system for non-administrative users, but nevertheless the access was restricted to root users as it is generally recommended.
- **Fixes:**
  - **Firewall rules regarding GRE and IPsec improved** — Automatic firewall rules in case of IPsec and/or GRE tunnels were improved and fixed. E.g., it is not possible to send unencrypted data (matching traffic selectors) out of M!DGE2 unit if the IPsec tunnel is down.
  - **Local IPsec IP address reset after any other IPsec change** — Local IPsec IP address was reset back to 0.0.0.0 if any other change had been made within this IPsec tunnel configuration. This was fixed.
  - **IP passthrough setup saved after clicking on the "Cancel" button** — Pressing the "Cancel" button within the IP passthrough setup does not apply the changes now.
  - **IPsec and OpenVPN default values after deleting particular VPN tunnel** — Default IPsec and OpenVPN parameters could be wrong after deleting a particular VPN tunnel.
  - **RRSP debug levels** — Debug level change for rrsp daemons was not applied immediately, but a reboot was required. It used to work only for rrsp2 daemon (Protocol server), but not for Terminal servers (rrsp11, rrsp12) and ModbusTCP (rrsp21) daemons.
  - **Put final END firewall rule after user defined rules** — The logical rule END which is added automatically is now inserted after all other rules.
  - **GUI improvements** — The loading time of web pages of the configuration interface was reduced.
    The password for DDNS service providers did not allow some special characters. This was fixed.
    On some GUI pages it was not possible to delete error and warning messages. This was fixed.
    The GUI mixed up the terms LAI (Location Area Identification) which contains MCC, MNC and LAC and PLMN (Public Land Mobile Network) which contains only MCC and MNC.
    The validation of the DHCP lease time input in the web interface was incorrect and changed to allow reasonable positive integers.
    Port based NAPT routing configuration could fail with an error message even though the configuration was technically correct. This was fixed.
    The initial password setup did not deny non-ASCII characters in the user password. Nevertheless, these characters were not handled correctly resulting in a device where the user could not log in. This was fixed. Now non-ASCII characters are rejected with an appropriate error message.
    A failure was fixed that prevented to set up ToS based extended routing filters.
    The web interface showed a misleading message when a new WWAN connection assigned a second SIM card to a WWAN module. The message was corrected.
    A WWAN network Scan always showed results linked to SIM1 even if another SIM was configured and used for the network scan. This was fixed.
    Not yet applied IPsec tunnel configurations could not be deleted via web interface. This was fixed.
    An Ethernet WAN link was not removed from the WAN link list if the corresponding Ethernet interface was bridged to another logical LAN interface. This was fixed.
    It was not possible to set client routes while the OpenVPN server was enabled. This was fixed.
    Some GUI input fields escaped HTML characters twice. This was fixed.
  - **SDK improvements** — Fixed memory leaks in MQTT message handler.
  - **IPsec aggressive mode tunnel establishment failed** — The option *i_dont_care_about_security_and_use_aggressive_mode_psk* was not set correctly.
  - **IP Passthrough Improvements** — In some rare condition the Client IP used for the Local IP Passthrough subnet could not be used. This was fixed with an optimized subnet allocation.

- **Configuration did not apply with FQDN IPsec peer** — Due to an invalid check on applying the new configuration, it could take several minutes until the configuration was processed. This was fixed.
- **IPsec with FQDN peer address not handled correctly** — The FQDN of the IPsec remote peer address was evaluated at configuration time and firewall rules were applied accordingly. This is not correct. The FQDN may resolve differently at run time and also the device may have no domain name service at configuration time at all. Now the FQDN is resolved at connection time.
- **CLI improvements** — The program version was printed incorrectly at program start. This was fixed.
  Sending a techsupport via email resulted in a crash of the CLI process. This was fixed.
- **Quagga BGP could not connect with PSK credentials** — The PSK credentials of Quagga were not processed correctly. This was fixed.
- **Single WWAN network configuration failed on Toby-L2** — It could happen that 2G- 3G- or 4G-only configurations did not connect to the network even though the network was available. This was fixed.
- **Low throughput on internal USB ports** — Some LTE modules did not show optimum performance as USB2.0 on some internal USB ports was not configured correctly. The configuration was fixed.
- **Bridged VLAN blocks broadcast packets** — The hardware switch chip drops VLAN tagged broadcast packets if a VLAN is bridged with an Ethernet interface. This was fixed by disabling the HW offload in such situations.
- **2nd DNS relay service does not work** — Configurations with different DNS relay servers for different interfaces did not work. This was fixed.
- **WWAN connection broken after switch from 2G-first to 4G-only** — It could happen that no WWAN connection came up after switching from 2G-first to 4G-only even though both networks were available. This was fixed.
- **Change of HTTP port failed** — It was not possible to change the server HTTP port. This was fixed.
- **IP passthrough failed** — In some situations, IP passthrough failed to propagate the IP settings correctly. This resulted in a reboot loop because the DHCP settings were considered invalid.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Discovery services** — Automatic discovery services (LLDP, CDP, …) do not operate correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.
  - **Auto refreshing some pages** — Once the change is applied, the process is started correctly. Settings are also saved successfully, but the process does not finish automatically. Refresh the page manually in such a case (e.g., changing LAN IP address).

Release 4.4.40.115, patch 1661

2023-04-11

Important

Upgrade M!DGE2 software to the latest 4.4.40.115 or 4.6.40.103 release together with Toby module firmware upgrade to the 17.00,A01.02 release. These upgrades mitigate an issue in which the Toby/WWAN module could get “missing” and was no longer possible to utilize cellular connection.

- **Fixes:**
  - **Modem reset via CFUN=15 during the M!DGE2 startup was disabled** — This issue together with Toby module firmware 17.00,A01.00 and 17.00,A01.01 could lead to serious state of ‘wwan module missing’ and a fix/replacement in RACOM RMA centre.
- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server’s mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Discovery services** — Automatic discovery services (LLDP, CDP, …) do not operate correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.114, patch 1627

2022-01-21

Note

Please be advised that the newly discovered vulnerability in the Apache Log4j logging framework with identifier CVE-2021-44228 does not affect any of the RACOM products, as we do not use Apache but Lighttpd http server in our products.

- **New Functionalities:**
  - **Support for password protected PKCS12 files in expert mode** — Expert mode configurations may now contain encrypted PKCS12 files. The passphrase needs to be provided together with the expert mode file.
  - **System downgrade to discontinued software releases disabled** — It is not possible to downgrade to software versions below 4.3.40.x. These software releases are out of service and it is not recommended to use them anymore.
  - **GUI improvements** — To configure local keys and certificates, it is mandatory to define a password for key encryption. If you did not do that, not very helpful error message appeared. The error message was improved.
    Message shown after web session timeout was improved.
    The module’s current firmware is displayed in the firmware update page as additional information.
- **Fixes:**

- **Fix of triggering sporadic watchdog reboots** — In the log files we received from a customer, we could see that the SMS daemon had triggered a system reboot. This is a very rare event which had its origin in a timing issue at the start sequence of the daemon.
- **Bridge netfiltering not set up correctly** — The global setting to enable bridge netfiltering was only applied if software bridge devices were present.
- **GUI improvements** — Enabling lldpd as solo activated discovery protocol produced an error message in the GUI. This was fixed.
  The web pages loading time of the configuration interface was reduced.
  Some configuration items were not reset to factory state when an OpenVPN connection was deleted. This was fixed.
  Received SMS could not be displayed in the web interface. This was fixed.
  It could happen that the web interface showed a misleading error message, while changes in bridge settings.
- **4G-only service type option** — It was not possible to connect to the cellular network if 4G-only service type is selected in 4.4.40.113 software version. This was fixed.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Discovery services** — Automatic discovery services (LLDP, CDP, …) do not operate correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.113, patch 1586

2021-09-21

- **New Functionalities:**
  - **Maximum number of static routes increased** — It is now possible to configure up to 50 static routes.
- **Security fixes:**
  - **CVE-2021-3712 OpenSSL Read buffer overrun** — The relevant bug-fixes for this issue were back-ported.
- **Fixes:**
  - **GUI improvements** — It was not possible to configure additional VRRP redundancy servers via web interface. This was fixed. Position of Edit and Delete button switched in IPsec tunnel configuration interface to match the normal work-flow.
    The SNMP MIB file download from the configuration web interface was fixed.
    It was not possible to configure additional VRRP redundancy servers via web interface. This was fixed.
    If a SIM card was removed, the web interface status showed "unassigned" instead of "missing". This was fixed.
    Spurious interface VOICE was removed from list of modules for firmware updates.
  - **Manual LAI (MCCMNC - PLMN)** — Change of allowed LTE provider's PLMN was fixed for Toby-L2 LTE modules.
- **Known Issues:**

- **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
  - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
  - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
- **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
- **Discovery services other than LLDP** — It is only possible to configure LLDP discovery protocol, others are not configurable.
- **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.112, patch 1578

2021-09-06

- **New Functionalities:**
- **Security fixes:**
  - **Linux Kernel Securtiy fixes** — CVE-2021-22555: Privilege escalation in Linux kernel allowed unprivileged users with shell access to gain root access or run a DoS attack on the system.
    CVE-2021-33909: Privilege escalation in Linux kernel allowed unprivileged users with shell access to gain root access.
- **Fixes:**
  - **No LTE connection with Toby-L2 with obsolete firmware version** — Toby-L2 LTE modules with Firmware 15.63 did not connect to mobile networks with Software 4.4.40.111. This was fixed. Nevertheless, it is strongly recommended to update the module firmware to the latest 17.00. Please ask our support if you need further advice.
- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Redundancy/VRRP** — It is not possible to enable Redundancy/VRRP.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Redundancy/VRRP** — It is not possible to enable Redundancy/VRRP.
  - **Discovery services other than LLDP** — It is only possible to configure LLDP discovery protocol, others are not configurable.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.111, patch 1559

2021-07-22

Important

Upgrade the Toby module version to 17.00,A01.00 before updating M!DGE2 Software to 4.4.40.111.
If installing 4.4.40.111 MIDGE2 software, make sure you have already upgraded Toby LTE module to newer version than 15.63 (i.e. 16.19,A01.02, 16.19,A01.04 or 17.00,A01.00)! Otherwise, the AT communication between M!DGE2 and the module stops working, which usually ends in a USB disconnection (i.e., MIDGE2/Toby LTE module cannot connect to cellular network).

Recommendation: Skip this Software version and use 4.4.40.112 or newer instead.

- **New Functionalities:**
  - **IPsec improvements** — It is now possible to disable Source-NAT rules for single IPsec SA's.
  - **GUI improvements** — It is now possible to disable Source-NAT rules for single IPsec SA's.
  - **SIM: Selecting bands manually did not work (Toby cellular modules)** — It is possible to select particular mobile bands now.
  - **Idle LTE Attach** — New config parameter *"modem.0.config.idle_lte_attach"*
    By setting the parameter to 0 [default]
    - M!DGE2 will force 2G/3G for a cellular modem bring up process and will apply the configured RAT (2G/3G/4G) a bit later. This is done to avoid unwanted data connections.

    By setting the parameter to 1
    - M!DGE2 will disable forcing "2G/3G-Only" mode during the bring up process. This can avoid issues especially in "4G-Only" modes. We could also see better behaviour with Manual LAI settings or Scan situations.
- **Security fixes:**
  - **Removing session login and logout cookies** — Existing login and logout session cookies of the web interface are now deleted. This reduces the potential risk of HTTP response splitting attacks or compromised web clients.
- **Fixes:**
  - **LTE connection issues** — In some situations, the Toby LTE modules disconnect and it takes several minutes until they re-connect. M!DGE2 detects these situations now and speeds up the reconnect time by sending a soft-reset command to the module. This reduces the reconnect-time substantially. It is also recommended to upgrade the module firmware.
  - **GNSS TCP server NMEA streaming error** — TCP clients which were not able to process all the received NMEA data from the server could disrupt the stream for other clients and lead to error messages on the router. This was fixed.
  - **"3G/4G only" preferred service-type** — This cellular connection option also allowed 2G/Edge connection. This was fixed.
- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Redundancy/VRRP** — It is not possible to enable Redundancy/VRRP.
  - **Discovery services other than LLDP** — It is only possible to configure LLDP discovery protocol, others are not configurable.

- **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.109, patch 1534

2021-06-11

- **New Functionalities:**
  - **GUI improvements** — The maximum CPU clock is increased from 600 MHz to 1 GHz, improving performance and throughput in several applications. CPU clock is adaptive (lower at high temperature and for low performance applications).
  - **TOBY LTE module firmware upgrade – version 17.00, A01.00** — Up-to-date Toby module FW is on our website in M!DGE2 download section and it is recommended to upgrade the module to
    - eliminate the risk of facing incompatibility issues with certain MNO networks [CA-90921]
    - and avoid loss of cellular connectivity in the event that MNOs dismiss legacy RATs (3G/2G) and CSFB service [u-blox ID 3501].

    Run the module FW upgrade from the menu “System – Modem Firmware Update” and choose “WWAN” module. Upload the FW to the unit. Upgrade can also be performed remotely via cellular network with several minutes’ connection drop. If you prefer, do the update via CLI.

    Make sure to use the correct FW for your particular module! Different firmware files are provided to Toby L200, L210 and L280 modules.
- **Security fixes:**
- **Fixes:**
  - **Web-Interface** — ITxPT and FMS2IP: licenses were shown as "not available" even in cases where they were actually available. This issue has been fixed.
  - **Misleading logging in situations with poor LTE coverage** — If the Toby LTE module lost connection to the network, the system logging showed errors in the AT command communication. The modem communication was fixed preventing failing commands.
  - **SDK improvements** — The example script *serial-tcp-broadcast.are* contained a semantic failure. This was fixed.
  - **Potential LTE connection loss** — Devices with Toby LTE modules occasionally lost LTE connection. This was persistent until M!DGE2 or the LTE connection is restarted, for example by the Link Supervision. It is recommended to properly configure Link Supervision if the device is supposed to work autonomously or if the WAN link is the only maintenance connection in the field application.
  - **GUI improvements**
    If an OpenVPN client was deleted via web interface, it could happen that the certificate association of other remaining OpenVPN configurations could be mixed up.
    Deleting firewall groups mixed up the order of groups.
    It was not possible to select UTC timezone together with daylight saving. This was fixed.
    Switching the interface of one VLAN from one LAN to another could fail in some situations. This was fixed.
    On edit of firewall rules, the wrong group was preselected. This was fixed.
    In some situations, the IPsec status shown in the web interface was wrong after connection loss.
    IPsec PSK handled ampersand character incorrectly. This was fixed.
    After a change of remote IP settings of an existing IPsec configuration, some firewall rules were not changed correctly. This was fixed.
    IPsec Common Name did not handle blank spaces correctly. Blanks are allowed now.
  - **IPsec dependent firewall rules not deleted if IPsec was disabled**
  - **GUI improvement** — PPTP was missing username and password fields in some situations.
  - **SDK improvements** — *nb_status("gnss").GNSS1_VERTICAL_SPEED* could crash the SDK host.

- **GSM calls not processed** — Sometimes incoming GSM calls were missed by the system. This was fixed.
- **Large techsupport files truncated** — It could happen to be incomplete due to missing disk space. This was fixed by not buffering the content.
- **IP packet loss on LTE modules** — IP packets with a specific length were lost on Transmission via LTE link on Toby LTE module in some rare situations. The USB communication was changed to fix this systematic failure.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **"3G/4G only" preferred service-type** — This cellular connection option also allows 2G/Edge connection.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Redundancy/VRRP** — It is not possible to enable Redundancy/VRRP.
  - **Discovery services other than LLDP** — It is only possible to configure LLDP discovery protocol, others are not configurable.
  - **Manual LAI** — Manual LAI configuration is available, but not working correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.107, patch 1495

2021-02-26

- **New Functionalities:**
  - **Higher M!DGE2 performance (HW Rev B02)** — The maximum CPU clock is increased from 600 MHz to 1 GHz, improving performance and throughput in several applications. CPU clock is adaptive (lower at high temperature and for low performance applications).
  - **SNMP improvements** — The SNMP EngineID is now configurable.
  - **GUI improvements & Toby module firmware update**
    A warning will alert the user if a WWAN module is running a firmware version which is known to be outdated and should be replaced with a newer one.
    Up-to-date Toby module FW is on our website in M!DGE2 download section. Run the module FW upgrade from the menu "System – Modem Firmware Update" and choose "WWAN" module. Upload the FW to the unit. Upgrade can also be performed remotely via cellular network with several minutes' connection drop. If you prefer, do the update via CLI.
  - **Additional status information on Toby-L2 LTE module** — The signal to noise ratio of the LTE connection is made available via CLI, SDK, SNMP and web interface.
- **Security fixes:**
  - **libmodbus security bug fix**
    CVE-2019-14463: out-of-bounds read fixed
    CVE-2019-14462: out-of-bounds read fixed
  - **OpenSSL security bug fix**
    CVE-2020-1971: Fixed NULL pointer deref in OpenSSL
  - **Security enhancement** — M!DGE2 web interface has been enhanced to be more robust against various XSS attacks. M!DGE2's bash CLI has also been hardened.

- **Fixes:**
  - **Switching between WWAN interfaces using two different SIM cards and one Toby module** — Switching between SIM1 and SIM2 profiles (within one Toby LTE module) was not possible in FWs 4.4.40.104 and 4.4.40.105. This was fixed.
  - **Password change did not apply on SNMP users** — In some situations, the SNMP user password was not applied with a change of the user's system password. This was fixed.
  - **/bin/login spamming logs** — On some devices it could happen that a failing call of /bin/login spammed the logs if no serial interfaces were configured as login console.
  - **SMS with a special "@" character** — No character in SMS after the 1st occurrence of "@" sign was sent. This was fixed.
  - **RS232 Login Console** — It was not possible to use the primary RS232 interface as Login console. This was fixed.
  - **GUI improvements**
    New table layout for Firewall menu. Clear button was deleted.
    Configurations with several IPsec tunnels which were configured with expert-mode could lead to wrong tunnel status shown in the web interface.
    GRE tunnel keys were treated like passwords in the web interface and shown as asterisks. This was wrong, because GRE tunnel key is not a secret, but only an identifier.
    Changing the shell of a user was not applied unless the user's current password was provided and changed at the same time. This was fixed. Now changing the shell of a user only requires the admin password for confirmation, but no user password or changed user password.
    The bridging status page was not accessible to non-admin users.
    The maximum file size for WWAN firmware-update files was increased to 45 MB. This should be sufficient to perform most FW updates directly via web interface without the need for an external web or FTP server.
    Setting the MTU of a bridge device BR1 or BR2 failed with an error message. This was fixed.
    The MTU was not applied correctly to soft bridge devices.
  - **Enable fast NTP synchronization after boot** — Due to a misconfiguration, the NTP client took up to 10 minutes to synchronize after the boot. This was fixed.
  - **L2TP tunnels cannot be bridged** — It was not possible to bridge L2TP tunnels to soft bridges BR1 and BR2. This was fixed.
  - **GUI: WPA-Enterprise Identity** — Setting the RADIUS identity had no impact to the configuration. The identity was always set to the hostname of the Router. This has been fixed.
  - **Local services not accessible with IPsec** — In some scenarios with multiple IPsec connections, it could happen that local services like the web interfaces were not available via IPsec. This was fixed.
  - **Unstable IPsec connection** — In some use cases with several parallel connections, IPsec was quite unstable due to timing issues on tunnel establishment. This was fixed.
  - **SMS not working with shared modem configuration** — SMS were not sent if the first WWAN interface was down even if the configuration was that the first available module should be used.
  - **Link management** — A bug in the dial-in behaviour on link-groups that resulted in preventing a switchover from happening was fixed.
  - **Mail transmission failures fixed** — Some MTA servers did not process mails with attachments from our SDK. This was due to a duplicate line in the mail header which is strictly not allowed in SMTP protocol. The duplicate line was removed.
  - **SNMP: missing MIB** — The HOST-RESOURCE-MIB was unsupported by the Router. This has been fixed.
  - **Reboot triggered by igmpproxy supervision** — The system health supervision failed on some igmpproxy setups resulting in a device reboot.
- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

    - Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **"3G/4G only" preferred service-type** — This cellular connection option also allows 2G/Edge connection.
  - **Too large techsupport files** — It is not possible to download correctly too large techsupport file. Sizes up to 50 MB are recommended.
  - **IPsec & XAUTH** — IPsec cannot be configured with XAUTH option.
  - **Redundancy/VRRP** — It is not possible to enable Redundancy/VRRP.
  - **Discovery services other than LLDP** — It is only possible to configure LLDP discovery protocol, others are not configurable.
  - **Manual LAI** — Manual LAI configuration is available, but not working correctly.
  - **WAN with STP/RSTP enabled** — It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

Release 4.4.40.105, patch 1447

2020-10-22

- **New Functionalities:**
  - **Port based DHCP addresses** — M!DGE2 supports port based DHCP address specification now.
  - **Certificate revocation list download for IPsec** — The IPsec daemon now tries to obtain the CRL file if a CRL location is defined in the installed certificate chain.
- **Security fixes:**
  - **Linux kernel security bug fixes**
    CVE-2020-8428: A use-after-free in the Linux kernel could allow local users to run a DoS.
    CVE-2020-10732: Uninitialized buffer might leak kernel data to user space on core dumps. The mainline bug fix was back-ported to the 4.4.40.x firmware.
    CVE-2020-12114: Possible denial of service by corrupted mountpoint reference counter. The mainline bug fix was back-ported to the 4.4.40.x firmware.
  - **Curl security bug fixes**
    CVE-2019-5482: A malicious TFTP server could cause a heap corruption in libcurl.
    Libcurl can be tricked to prepend a part of the password to the host name before it resolves it, potentially leaking the partial password over the network and to the DNS server(s).
    CVE-2019-5436: Possible TFTP receive buffer overflow fixed.
    CVE-2019-5435: libcurl contains two integer overflows which if triggered can lead to a too small buffer allocation and a subsequent heap buffer overflow.
- **Fixes:**
  - **Firewall rule blocked IPsec traffic from router** — In setups where all traffic but IPsec is blocked it could happen that packets from the router were unintentionally blocked as well, even though they were supposed to be sent via IPsec. This was due to a missing firewall rule that was present for forwarded traffic, but was missing in the outgoing chain.
  - **GUI improvements**
    The web interface did not allow to disable Dead Pear Detection (DPD). This was fixed.
    Due to a flaw in the GUI design it could happen that firewall rules could not be edited or deleted via web interface. This was fixed.
    The web interface enforced the first WWAN interface to be permanent. This restriction was not needed and therefore removed.

- **M!DGE2 services cannot be accessed via IPsec** — An issue with packet fragmentation prevented to access services (like web interface or SSH access) via IPsec. Routed data traffic was not affected. This issue was fixed. If you relied on this malicious behaviour as a feature, you should get in contact with our support to find a valid firewall configuration.
- **Multicast packets, GOOSE, Profinet data not forwarded on M!DGE2** — Starting with FW release 4.3.40.100 multicast IP packets were not forwarded on switched Ethernet ports of M!DGE2. This was fixed.
- **No default route on WWAN with custom APN** — There was a customer setup with a private APN where we failed to establish the default route over WWAN. The issue was fixed. Working APN setups are not affected by the fix.
- **CLI improvements** — The CLI status did not show SWI information for the second PDP context.
- **SCEP enrolment did not work with Windows PKI** — Certificates provided by a Windows PKI were not installed correctly. This has been fixed.
- **Certificate chains from SCEP server** — Certificate chains installed via SCEP did not work with IPsec.
- **IPsec tunnel, wrong IP Source address** — In a specific situation with multiple WANs and dynamic routing, it could happen that M!DGE2 could try to establish an IPsec tunnel with a wrong source IP address (from a wrong WAN interface). This was fixed.
- **BGP, IPsec default parameters** — Most of default parameters were changed to match the default values in RipEX2 radio.
- **AT commands failure** — In some rare situations, internal AT commands could be handled wrongly. This was fixed by a new Toby module firmware 16.19. Contact our support team for a download link.
- **STP is disabled by default** — STP could cause some troubles if not configured correctly within the network. STP was disabled by default, but it is possible to configure it and use it on LAN interfaces.
- **Telnet is disabled by default** — Telnet is disabled by default. SSH is suggested to be used.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.
  - **Switching between WWAN interfaces using two different SIM cards and one Toby module** — Switching between SIM1 and SIM2 profiles (within one Toby LTE module) is not possible in FWs 4.4.40.104 and 4.4.40.105. For such functionality, please use FW 4.4.40.101.

Release 4.4.40.104, patch 1416

2020-05-14

- **New Functionalities:**
  - **IPsec improvements** — IPsec tunnels can be enabled and disabled individually now.
  - **Prevent down-grade to incompatible version** — If you want to downgrade to an older release, you may have to install intermediate releases. Normally that's the latest release of the major version of the desired software. The Update process will detect the release number of the uploaded image and prevent installation of invalid releases.
  - **IPsec** — The number of configurable IPsec tunnels was increased to 10.
  - **GUI improvements**

It is now possible to configure whether status messages should appear on the web interface login page.
The system log level settings can now be changed more convenient in the web interface.
It is now possible to import IPsec expert mode files with encrypted keys via the web interface.
Routers with Toby-L2 LTE modules now show LTE band information on the WWAN status page.

- **SDK improvements** — M!DGE2 can now be set to a low power sleep mode from SDK.
- **STP and RSTP** — STP and RSTP is now supported.
- **Improved user access rights** — The user access management was improved. It is now possible to grant native shell access to additional admin users or to disable shell access for a user.
- **Additional GRE tunnel parameters** — It is now possible to configure tunnel keys for GRE to allow a gateway to distinguish between GRE packages from different connected end devices.
- **Additional BGP settings** — The BGP setup allows to configure additional parameters for time-out, hold-time and weight.
- **Maximum number of static DHCP hosts increased** — It is now possible to configure up to 70 static DHCP host entries.
- **Asymmetric routing is available** — Asymmetric routing is when a packet takes one path to the destination and takes another path when returning to the source. These data were dropped by M!DGE2 firewall. It could cause temporary issues if RipEX Backup paths were configured in the network. It can be controlled now via CLI. The required parameter is “firewall.invalid_ip”.

- **Security fixes:**
  - **Security fixes in 3rd party and open source packages**
    CVE-2018-15599: dropbear contained a user enumeration vulnerability
    CVE-2020-8597: pppd remote code execution in EAP code
- **Fixes:**
  - **ublox Toby-L2 SMS handling** — While receiving big SMS messages, the evaluation of the SMS message index could lead to wrong results.
  - **IPsec tunnel configuration failed** — It could happen that IPsec was not correctly activated after installing a user-configuration file. This could happen with special configuration settings. If IPsec came up after applying a configuration (most scenarios), then you were not affected.
  - **GUI improvements**
    The required RSSI value for mobile interfaces was set to 100 dBm automatically without customer interaction.
    NTP Server did not allow to set up access from world (0.0.0.0/0).
    IPsec network configuration allows to configure overlapping networks for local and remote side now.
    File format of tcpdump debug traces from the web interface was improved.
    It could happen that a software update failed with a generic error message if the software image download failed. Now, in such cases, the web interface will show a more helpful error message.
    It was not possible to configure a firewall rule with dedicated incoming and outgoing interface.
    The web interface returned an error if some special characters like quotes were used inside an email password.
    Disabled radio buttons where not shown as disabled. Nevertheless, it was not possible to change their values.
    Logs from SDK scripts did not wrap with the page width of the web interface.
  - **ublox Toby-L2 I^2S communication** — The I^2S communication could fail while using a ublox Toby-L2 module.
  - **Toby-L2 initial registration** — While using a Toby-L2 module, the initial registration could fail when no 2G connection was available.
  - **Authentication in SMS control SDK script** — The SMS control SDK script which is enabled by default in every M!DGE2 unit did not accept the ‘admin’ password until un-storing and storing its password was done. For all already configured M!DGE2 units, a factory-reset must be applied for the functionality to be fully operational or that unstore/store procedure.

- **Software downgrade via USB stick failed** — In factory state, the downgrade to Releases prior 4.2.40.x failed.
- **SDK improvements** — The function nb_syslog() did not clean an internal buffer correctly which could lead to corrupted log messages.
  Due to an erase condition, mails sent from the SDK on a high rate could get lost before they were sent.
- **Possible LTE connection loss** — Devices with Toby-L2 LTE modules faced sporadic connection losses. In some cases, the connection could not be re-established until reboot. This was fixed.
- **Bring up several LTE connections with switch-over links** — Switch-over links should come up if their permanent master link disconnects. This did not work correctly if there were several permanent WWAN links with switch-over configured.
- **Configuration via USB stick could fail** — Due to a time-out issue, it could happen that consecutive configuration steps via USB stick failed. This would only affect you if you use one USB stick with some base configuration and then apply another configuration with a USB stick on top without rebooting between these steps. You can apply consecutive configurations via USB stick one after the other now.
- **IPsec improvements** — In some situations, it was not possible to reach the configuration web interface of a local router because traffic was erroneously routed via the IPsec tunnel. This was fixed.
- **Link supervision timeout prevents switch to better link** — If link supervision was enabled, the link management did not change to a better link before the supervision timeout was reached. Even if the link was obviously down. This was changed so that a better link would be taken into account directly once being sure the old one was lost.
- **Low LTE throughput** — Due to a failure in the TCP window management, the LTE throughput was very low. This was especially an issue in longer TCP sessions like big file downloads or VPN connections.
- **USB-Ethernet adapter not working** — Due to an internal misconfiguration, USB-Ethernet adapters were not shown in the IP setup of the web interface.
- **Reset of GNSS module could fail** — There had been situations where the GNSS supervision failed to reset a GNSS module correctly. In that case, no GNSS fix was available until the next system reboot.
- **Installing a software release could lead to loss of stored factory configuration** — After installing a new software release, the factory configuration manually stored by the customer was lost.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

Release 4.4.40.101, patch 1354

2019-12-12

- **New Functionalities:**
  - **GUI improvements**
    Redundant settings for HTTP, HTTPS and telnet were removed. These services are now managed via Services setup.
  - **SDK improvements** — New function usleep() provides sub second sleep intervals.
    New API function to nb_syslog_p() for logging to different log levels.

- **GNSS dead-reckoning** — New configuration options to store and load GNSS DR calibration data to the GNSS module for faster DR learning and better DR data basis.
- **SNMP service improvements** — System temperature is now provided on SNMP poll. The OID is 1.3.6.1.4.1.33555.10.40.50.0.
- **Added support for certificate chains for OpenVPN export mode configuration** — It is possible now to install certificate chains for OpenVPN using the expert mode configuration process.
- **Netflow interface supervision for Ethernet and WWAN interfaces** — Netflow was introduced for WLAN interfaces and is now available for other device types like Ethernet and WWAN as well.
- **MQTT Broker** — A MQTT Broker can now configured on M!DGE2 Routers providing MQTT service to the network.
- **Key-parameter support for GRE tunnels** — GRE tunnels now support the Key-parameter which is used to separate different GRE tunnels between two end-points.

- **Security fixes:**
- **Fixes:**
  - **Watchdog on failing SDK script did not work** — A change in the watchdog API was not properly handled by the SDK scripting engine. Resulting in watchdog to fail to restart the System on error. This was fixed.
  - **Problems on switch-over between WAN and WWAN** — Under rare conditions, the switch over between WAN and WWAN did not work as expected.
  - **GUI improvements**
    The GUI failed to set some special characters like '&'.
    If VLAN is configured on bridge devices, the bridge interfaces showed up several times in the web GUI. This was fixed.
    Due to a mistake in the input sanity check, it was not possible to change some user options without changing the user's password. This was fixed.
    For actions which require the current password which is normally stored only as salted hash, it is still required to provide the password, but this (new) password may be the same as the old one.
    Due to a failure in string escaping functionality, some AT commands failed. This was fixed.
    Fixed typo
  - **IPsec tunnels failed to start** — Due to timing issues on setups with several IPsec tunnels, some of these sometimes failed to start. The start procedure was changed to prevent this failure.
  - **Old configuration files failed to apply** — Some very old configuration files failed to apply with error message 'Unable to create backup'. This was fixed.
  - **Bridge interface lost on software update** — Software bridge interfaces (like BR1, BR2) might get lost on SW-Update and needed to be reconfigured after the update was finished. This was fixed and the bridge interfaces are preserved on software update.
  - **Storage date of last "Factory Default Config" is not updated on consecutive storage events** — If the function to store the current configuration as factory default is called several times, the timestamp of the latest store event is not updated. This was fixed.
  - **SDK improvements** — nb_dio_count failed to remove obsolete data resulting in wrong data. This was fixed.
  - **GNSS data show up delayed** — We have seen GNSS data to be delayed by some seconds due to a failure in buffer handling. This was fixed.
  - **4G-only WWAN connection failed to connect** — Under certain conditions, LTE modules failed to connect if 4G-only was selected even through LTE network was available. That was fixed.
  - **Unstable WWAN connection with LTE-First setting** — With LTE-First option, some LTE modules failed to establish connection under poor LTE conditions on software release 4.3.40.102. This was fixed.
  - **The LTE module could stay in 2G or 3G even though better service type is available** — This has been fixed.
  - **Connection tracking for FTP service missing** — On software releases since 4.3.40.100, the connection tracking for FTP was not configured correctly. This was fixed.

- **TCP/IP connection not established when the connection is terminated inside M!DGE2 router** — This was fixed by changing of internal kernel parameters.
- **Reboot with GNSS module** — The GNSS module in combination with 4.3.40.x causes rebooting of the M!DGE2 unit. This was fixed.
- **Boot order of services** — In some rare combination of M!DGE2 services, the particular service did not come up correctly. The order of services has been improved.
- **TCP establishment** — Some TCP sessions (ports) could not be fully established if this TCP was terminated in M!DGE2 while GRE over IPsec was established. This was fixed.

- **Known Issues:**
  - **Protocol server restrictions** — The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:
    - Only one Protocol server can be configured even in units with more RS232 interfaces.
    - If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to the 1st LAN IP address of local M!DGE2). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

