Release notes MCX8 Firmware

Firmware 3.14t → 3.14u (29.07.2024)

Security updates:

Update of the Linux kernel version from 6.1.81 → 6.1.100

Functional changes:

1. SCEP: Fingerprint extended by SHA256 and SHA512
2. mDNS and LLMNR forwarding for IPv6 packets
3. Relay control now also with IPv6
4. GPS Handler now with IPv6 support

Bugfix:

1. Relay status: error when accessing /API/Status/Relay directly
2. With the current OpenSSL version, the verification of some certificates no longer worked.
3. DHCP server: when the list of IPs to be assigned is exhausted, the oldest entries are now automatically removed from the "Reserved List" and then reassigned.

Firmware 3.14s → 3.14t (10.04.2024)

Functional changes:

1. Display of Captive Portal if the DHCP client was supplied with option 114 by the DHCP server.
2. LTE/5G: Service domain can be set (CS&PS, CS, PS)

Bugfix:

1. Roaming/Score: Bugfix for TPC rating for APs transmitting on 5GHz channels >= 128. Under certain circumstances it could happen that APs with low SNR value were rated higher than APs with a higher SNR.
2. Login form with background blocking (CDC) - After more than 5 seconds, it was no longer possible to log in with read-only users.

Firmware 3.14r → 3.14s (19.03.2024)

Security updates:

Update of the Linux kernel version from 6.1.70 → 6.1.81
OpenSSL update to version: 3.2.1 (30 Jan 2024)

Functional changes:

implemented EST as an additional method for certificate distribution and updating
ping test: Adjustable parameter "Short Interval", which defines the shortened ping interval after an AP change.

update for the WPA supplicant: git 6777ff62
4th MQTT client: Server Name Indicator (SNI) added for TLS connections.

Bugfix:

1. deleting all dump and log files could cause the firmware to crash

Firmware 3.14p → 3.14r (10.01.2024)

Security updates:

Update of the Linux kernel version from 6.1.51 → 6.1.70
OpenSSL update to version: 3.1.4

Functional changes:

1. SCEP: Challange variant now also possible with V_ASN1_UTF8STRING.
2. SCEP: RFC 5652: Cryptographic Message Syntax (CMS) implemented
3. WLAN-Dump: new option for selecting what is to be recorded:
   moni0 → (Wireless Header)
   wlan0 → (Ethernet Header)
4. DNS forwarding: now with active handling instead of simple forwarding.
5. The Network Test website now also supports IPv6
6. Pseudo Level2 Bridge Mode: the client IP is now also "learned" from received ARP packets.
7. Reverse lookup of the host name via WLAN IP is now possible
8. MQTT Client + Serial can communicate via IPv6.
9. VPN: IPSec extended and WireGuard® added

Firmware 3.14o → 3.14p (18.10.2023)

Security updates:

Change Linux kernel version from 6.1.44 → 6.1.51
Buildroot: Move to OpenSSL 3 (OpenSSL 3.0.11 19 Sep 2023).

Functional changes:

1) input status: the status is displayed on the web page (Home) and can be queried via the API.
2) API/Status/Wireless.Connection Information for LANCloning adapted.
3) new element "Encryption" in "/API/Status/Wireless/Accesspoints/xx".

Firmware 3.14n → 3.14o (25.08.2023)

Security updates:

Change Linux kernel version from 6.1.36 → 6.1.44

Functional changes:

1. SYN flood detection increased to 40 SYN burst. On average 5 SYN / second is still ok.
2. SNMP: Addition of status values from the info of /proc/net/dev
3. Improvement for IPv6 bridging

4. SCEP: If the CA Identity parameter for the URL contains illegal characters the value is URL-Encoded
5. Display of additional warnings in MCConfig (from Vers.: 2_0_3_9) in the column "Status":
   - For certificates that are about to expire or have already expired.
   - For incorrectly configured ping test.
6. After a "reset to defaults" of the config via the web interface or also when uploading a configuration, the view automatically changes to the configuration web page after 2 seconds.

Firmware 3.14m → 3.14n (24.07.2023)

Security updates:

Change Linux kernel version from 6.1.33 → 6.1.36

Functional changes:

1. Web server security:
   - Preferences for the TLS session handshake algorithms can now be set.
   - New option Send HSTS header
2. EAP: EAP-TTLS can now also be performed without certificates. (similar to EAP-PEAP)
3. Wireless: wpa_supplicant now with 802.11v support.
4. Wireless: now shows in the AP list whether an access point supports 802.11v.
5. Serial: The serial interface can now also communicate via TLS.
   Certificates for authentication can also be installed for this purpose
6. Bridge/NAT: now with warnings for conflicts of local services of the device with NAT rules defined by setup.
7. MQTT Bridge: Now also with local web socket port (default 8080)

Firmware 3.14k → 3.14m (06.14.2023)

Security updates:

Change Linux kernel version from 6.1.23 → 6.1.33

Functional changes:

1 wpa_supplicant updated to 2.11-dev (Git Rev. 95C3f0d1)

2 Improvement in relay control via the
Erroneous sequences and relay commands are now rejected with HTTP Error 400.

3 Output a warning in the debug log if all matching SSID's are evaluated with 0 during the score calculation. This indicates that one of the crypto settings does not fit.

4 Warning in debug log after startup if certificates (client and CA certificates) are loaded that are about to expire or have already expired.

Firmware 3.14i → 3.14k (16.05.2023)

Functional changes:

1. The relay is now also controllable via the REST API and using statement sequences.
2. Authentication of individual API/URLs:
   This makes it possible to secure access to certain API functions with a separate user/password without having to use the user/password for the device configuration.
3. 5G/LTE: Firmware update support for RM520N-GL

Bugfix:

Fixed segfault error in MQTT function (TLS write)
Segfault error in timer module fixed (Blacklist + ConfigChange)