

Release notes MCX8 Firmware

Firmware 3.15.4 → 3.15.5 (31.03.2026)

Functional changes:

- 1 Bridge Mode:
 - MAC authentication is now also available in L2 pseudo-bridge mode

Bug fixes

- 1 Serial:
 - Fix for the timeout trigger (only faulty in version 3.15.4)

Firmware 3.15.3 → 3.15.4 (25.03.2026)

Security updates:

Update of the Linux kernel version from 6.1.158 → 6.18.18
BuildRoot 2025.11.3 (Git Rev. ffbffaea, OpenSSL 3.6.1)

Functional changes:

- 1) Wireless:
 - OKC (Opportunistic Key Caching) can be configured in the Wi-Fi profile.
 - The maximum number of channels scanned during the background scan for targeted roaming is now configurable (previously fixed at 4).
 - 802.11w is configurable for all configurations that include WPA3.
 - PMK Lifetime can be configured.
- 2) NAT/Single Client NAT:
 - Rules for incoming data not only for WLAN but also for tunnel interfaces.
- 3) Wireguard:
 - Visibility in MCConfig with WireGuard IP and status on the website.

Bug fixes

- 1) Wireless/Mesh:
 - It now works with encryption as well.

Firmware 3.15.2 → 3.15.3 (09.12.2025)

Security updates:

Update of the Linux kernel version from 6.1.155 → 6.1.158
BuildRoot 2025.02.8 (Git Rev. 8215c5de)
wpa_supplicant update to current developer git version.

Functional changes:

- 4) Introduction of a new parameter for serial -> with UDP mode:
 - You can now specify a "backup server IP" in case the "server IP" fails.

- 5) Wireless: For EAP, the minimum requirement for the TLS version used is now configurable.
- 6) DHCP client: The transaction IDs used for DISCOVER are now stored for longer so that delayed responses from the DHCP server can be taken into account.
- 7) API: Various system variables can be queried using the "/API/Status/System/StateVars" query.
- 8) IPSec: New Site-2-Site mode added.

Bug fixes

- 1) Fix: When switching bridge modes, the parameter check might have reported an error that was not relevant in the new mode. For example, the IP range of the DHCP server was reported as incorrect even though the DHCP server was switched off.
- 2) NTP server on the LAN side did not work when using NTS.

Firmware 3.15.1 → 3.15.2 (14.10.2025)

Security updates:

Update of the Linux kernel version from 6.1.145 → 6.1.155
BuildRoot 2025.02.6 (Git Rev. 6360671c)

Functional changes:

- 9) Revocation Checking of certificates via OCSP and CRL implemented. Rejection only occurs if a revoked status has been explicitly determined.
- 10) NAT with MAC Authentication: All IP addresses specified in the NAT rules are now checked via ARP to see if they are accessible. This also allows passive clients to be detected.
- 11) NAT: MAC authentication: Now compatible with CISCO® requirements for MAC authentication bypass (MAB).
- 12) NAT: DNS suffix delegation: You can now specify special DNS server addresses for certain domains.
- 13) NAT: DNS server + forwarder information now available via API:
/API/Status/Network/DNS
- 14) Wireless: SuiteB-192 implemented as an additional encryption mode.

Bug fixes

- 1) Visibility in MCCConfig via IPSec assigned IP / vti1 interface given
- 2) SCEP: CA certificate was not reliably imported in all configurations.
- 3) SCEP: Now not only the fingerprint but also loaded CA certificates are trusted.

Firmware 3.14y → 3.15.1 (28.07.2025)

Security updates:

Update of the Linux kernel version from 6.1.130 → 6.1.145
BuildRoot 2025.02.4 (Git Rev. 00d5d387)

Measures for compliance with the requirements of EN 18031 / RED-DA

- 2 Display of warnings when using insecure encryption methods
- 3 User/password must be set to activate the bridge functionality.

- Data for controlling the relay and the serial interface are also affected. This situation is indicated by rapid orange/light blue flashing of the power LED
- 4 The user can now set up an update server via which firmware updates can be automatically distributed to the MC devices.
 - 5 An audit log file is now also kept, which cannot be deleted.
 - 6 Warnings for unsafe settings
 - 7 Default parameters only with secure settings
 - 8 Reject firmware downgrades when secure settings are active
 - 9 HTTP Digest authentication can now be used for the API.
 - 10 The firmware is secured with an additional signature (SHA512 + secp521r1)
 - 11 IDS (Intrusion Detection System):
Limits of SYN/RST/Unrelated/Invalid and PING with blocking of the attacker's IP
Web interface/API/Config tool with limiting of attempts through increasing attempt intervals
 - 12 Time synchronization with improved security: NTS as an extension of the NTP protocol.
With secure time information via NTS, expired CA certificates are removed from the configuration
 - 13 Config-Stick support removed. This functionality is not compatible with EN18031

Functional changes:

- 2 Measurement and display of the temperature measured by the CPU (CPU chip temperature)
- 3 Web interface: Button for displaying passwords when entering them
- 4 MQTT: Improvements when connection is terminated. Display of in-flight message count on disconnection
- 5 SSID profile: Ignoring the CA certificate check now possible via explicit setting
- 6 Roaming Control API: Scan all channels if only ?Cmd=Scan without channel is called.
- 7 Wireless roaming→Pingtest: Reconnect can also be performed multiple times. Reconnects are repeated at intervals of 2, 4, 8 or 16 times, based on the configured number, so that a repeated reconnect may lead to a solution to the problem
- 8 CA certificates are now only stored centrally and no longer per function in the configuration
- 9 Firmware numbering changed. No more letters but numbers
<Main>.<Sub>.<Minor>[.<Patch>[-RC<Num>]]

Bugfix:

Problem with read-only user with secured MConfig communication fixed.

Firmware 3.14x → 3.14y (25.04.2025)

Security updates:

Update of the Linux kernel version from 6.1.130 → 6.1.134
BuildRoot 2024.11.3 (Git Rev. 8fdf9ed8)

Functional changes:

1. Relay:
 - If the relay is controlled via MQTT, access via a UPS port can now also be activated.
 - Previously, the control commands for switching on and off were strictly checked not only for the correct content but also for the exact length. Now subsequent zero bytes + CR+NL+TAB are tolerated.
2. IPV6:
Improvement in IPV6 bridging
3. Roaming
ARP test implemented as an alternative method to the ping test.

Bugfix:

- 14 NAT:
Forward multicast packets from LAN → WLAN were sent with an incorrect checksum.
- 15 Wireless Scan:
Under certain circumstances, it could happen that no more scans took place at times.
- 16 Config:
Errors could occur with some setting options, especially if several instances could be created. (e.g. serial interfaces, SSID profiles)

Firmware 3.14w → 3.14x (17.03.2025)

Security updates:

Update of the Linux kernel version from 6.1.119 → 6.1.130
OpenSSL Update to 3.4.1 (11 Feb 2025)

Functional changes:

1. Serial:
 - Improvement of the timeout condition for the send trigger
 - Network Mode: REST API added. Data can now also be sent and received via the web server.
 - Handshake mode XON/XOFF bytes in the output buffer are now adjustable.
2. Admin→Webserver :
 - Certificate now selectable
 - Option for the interface via which the web server can be reached:
→ LAN only or LAN+WLAN+LTE/5G
3. Wireless: Special handling for mode: FT and SHA256 in combination
4. Relay: Control of the relay via MQTT now also with JSON data

Bugfix:

1. LAN client cloning mode: Unicast sent DHCP requests now with correct destination MAC.

2. dropping of packets INVALID/UNTRACKED (Leaky NAT)
3. Relay: Warning for PhraseOff = "" (empty) removed.

Firmware 3.14v → 3.14w (27.11.2024)

Security updates:

Update of the Linux kernel version from 6.1.105 → 6.1.119
OpenSSL Update to 3.3.2.3 (Sep 24)
WPA_Supplikant Update to 2.12

Functional changes:

- 1) IPv6 Support added for:
SNMP-Server
NTP-Client
Wireless Info Output
AUX-Input
- 2) Home → Extended status information for the WLAN interface:
TX and Rx bit rate are now displayed separately.
“channel usage” display now also in the 6GHz band
- 3) API status now also with WLAN MAC information
- 4) NAT: Forwarding of Bcast/Mcast can be activated
- 5) SCEP: SAN configurable, CN with wildcard support
- 6) Wireless Info string now also with %wlanipv6
- 7) Encrypted communication between MC and MCConfig program can now be permanently activated (Admin → Configuration tool accessibility). However, this only works when using an MCConfig program version $\geq 2.0.3.17$
- 8) NTP server: If the NTP client function is activated and DHCP is active, an NTP server IP is now also requested. The NTP server IP provided in the DHCP response is then entered where the “NTP server” or “Backup NTP server” parameter is set to 0.0.0.0.

Firmware 3.14u → 3.14v (19.08.2024)

Security updates:

Update of the Linux kernel version from 6.1.100 → 6.1.105
OpenSSL update to 3.3.1.4 (June 24)
WPA_Supplikant update to 2.11

Functional changes:

4. Previously, only 4 CA certificates per function (wireless, MQTT ...) could be stored on the MC devices. Now many CA certificates can be uploaded if required. It is recommended to keep the number of uploaded certificates low. There should not be more than 150 certificates in total (wireless, MQTT, serial). Version $\geq 2.0.3.16$ must be used to manage the certificates via MCConfig.

Bugfix:

- 17 The SNMP module responds to requests again.

Firmware 3.14t → 3.14u (29.07.2024)

This version was withdrawn because the SNMP function no longer worked with it.

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:

4. Relay status: error when accessing /API/Status/Relay directly
5. With the current OpenSSL version, the verification of some certificates no longer worked.
6. 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: Challenge 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 MConfig (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:

- 10 wpa_supplicant updated to 2.11-dev (Git Rev. 95C3f0d1)
- 11 Improvement in relay control via the
Erroneous sequences and relay commands are now rejected with HTTP Error 400.
- 12 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.
- 13 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:

- 18 The relay is now also controllable via the REST API and using statement sequences.
- 19 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.
- 20 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)