

Release notes MCX8 Firmware

Firmware 3.14v → 3.14w (27.11.2024)

Sicherheits-Updates:

- Update der Linux Kernel Version von 6.1.105 → 6.1.119
- OpenSSL Update auf 3.3.2.3 (Sep 24)
- WPA_Supplikant Update auf 2.12

Funktionelle Änderungen:

- 1) IPv6 Support hinzugefügt für:
SNMP-Server
NTP-Client
Wireless Info Ausgabe
AUX-Input
- 2) Webseite Home → erweitere Statusangaben für das WLAN-Interface:
TX und Rx Bitrate wird jetzt getrennt angezeigt.
„channel usage“ Anzeige jetzt auch im 6GHz Band
- 3) API status now also with WLAN MAC information
- 4) Forwarding von Bcast/Mcast kann aktiviert werden
- 5) SCEP: SAN konfigurierbar, CN mit Wildcardunterstützung
- 6) Wireless Info string jetzt auch mit %wlanipv6
- 7) Die verschlüsselte Kommunikation zwischen MC und MCCConfig-Programm kann jetzt fest aktiviert werden (Admin → Configuration tool accessibility). Dies funktioniert aber nur bei Verwendung einer MCCConfig Programmversion $\geq 2.0.3.17$
- 8) NTPServer: Bei aktivierter NTP-Client-Funktion und aktivem DHCP wird jetzt auch eine NTP-Server-IP angefragt. Die in der DHCP-Antwort mitgeteilte NTP-Server-IP wird dann dort eingetragen, wo der Parameter „NTP-Server“ oder „Backup NTP Server“ auf 0.0.0.0 gesetzt ist.

Firmware 3.14u → 3.14v (19.08.2024)

Sicherheits-Updates:

- Update der Linux Kernel Version von 6.1.100 → 6.1.105
- OpenSSL Update auf 3.3.1.4 (Juni 24)
- WPA_Supplikant Update auf 2.11

Funktionelle Änderungen:

- 9) Bisher konnten nur 4 CA-Zertifikate pro Funktion (Wireless, MQTT ...) auf den MC-Geräten gespeichert werden.
Jetzt können bei Bedarf viele CA-Zertifikate hochgeladen werden. Es wird empfohlen die Anzahl der geladenen Zertifikate gering zu halten. Mehr als 150 Zertifikate sollten es in Summe (Wireless, MQTT, seriell) nicht sein. Zur Verwaltung der Zertifikate per MCCConfig muss die Version $\geq 2.0.3.16$ eingesetzt werden.

Bugfix:

1. Das SNMP-Modul antwortet wieder auf Anfragen.

Firmware 3.14t → 3.14u (29.07.2024)

diese Version wurde zurückgezogen, weil die SNMP-Funktion damit nicht mehr funktionierte.

Sicherheits-Updates:

Update der Linux Kernel Version von 6.1.81 → 6.1.100

Funktionelle Änderungen:

1. SCEP: Fingerprint um SHA256 und SHA512 erweitert
2. mDNS und LLMNR: Durchleitung von IPv6 Paketen
3. Relais-Ansteuerung jetzt auch mit IPv6
4. GPS Handler jetzt mit IPv6 Support

Bugfix:

1. Relais-Status: Fehler bei direktem Zugriff auf /API/Status/Relay
2. Mit der aktuellen OpenSSL Version funktionierte die Prüfung einiger Zertifikate nicht mehr.
3. DHCP-Server: wenn die Liste der zu vergebenden IP's aufgebraucht ist, werden jetzt automatisch die ältesten Einträge aus der „Reserved List“ herausgenommen und dann wieder neu vergeben.

Firmware 3.14r → 3.14s (19.03.2024)

Sicherheits-Updates:

Update der Linux Kernel Version von 6.1.70 → 6.1.81
OpenSSL update to version: 3.2.1 (30 Jan 2024)

Funktionelle Änderungen:

1. EST als weitere Methode zur Zertifikatsverteilung und Aktualisierung implementiert
2. PingTest: Einstellbarer Parameter „Short Interval“, der den verkürzten Ping-Intervall nach einem AP-Wechsel festlegt.
3. Update für den WPA-Supplimenten : git 6777ff62
4. MQTT-Client: Server Name Indicator (SNI) bei TLS-Verbindungen hinzugefügt.

Bugfix:

1. Beim Löschen aller Dump und Log-Dateien könnte es zu einem Absturz der Firmware kommen

Firmware 3.14p → 3.14r (10.01.2024)

Sicherheits-Updates:

Update der Linux Kernel Version von 6.1.51 → 6.1.70
OpenSSL update auf Version: 3.1.4

Funktionelle Änderungen:

1. SCEP: Challenge Variante jetzt auch mit V_ASN1_UTF8STRING möglich.
2. SCEP: RFC 5652: Cryptographic Message Syntax (CMS) implementiert

3. WLAN-Dump: neue Option zur Auswahl was aufgezeichnet werden soll:
 moni0 → Wireless Header (mit 802.11 Traffic)
 wlan0 → Ethernet Header (ohne 802.11 Traffic)
4. DNS-Forwarding: jetzt mit aktivem Handling anstelle von einfachem Weiterleiten.
5. Die Webseite Network Test unterstützt jetzt auch IPv6
6. Pseudo Level2 Bridge Mode: die Client IP wird jetzt auch aus empfangenen ARP-Paketen „gelernt“.
7. Reverse Lookup des Hostnamens über WLAN-IP ist jetzt möglich
8. MQTT Client + Seriell können über IPv6 kommunizieren.
9. VPN: IPSec erweitert und WireGuard® hinzugefügt

Firmware 3.14o → 3.14p (18.10.2023)

Sicherheits-Updates:

Wechsel der Linux Kernel Version von 6.1.44 → 6.1.51
 Buildroot: Umstieg auf OpenSSL 3 (OpenSSL 3.0.11 19 Sep 2023)

Funktionelle Änderungen:

1. Input-Status: Der Status wird auf der Webseite (Home) angezeigt und kann über die API abgefragt werden.
2. API/Status/Wireless.Connection: Information für LANCloning angepasst.
3. neues Element „Encryption“ in „/API/Status/Wireless/Accesspoints/xx“

Firmware 3.14n → 3.14o (25.08.2023)

Sicherheits-Updates:

Wechsel der Linux Kernel Version von 6.1.36 → 6.1.44

Funktionelle Änderungen:

SYN-Flood Erkennung auf 40 SYN Burst heraufgesetzt. Durchschnittlich sind 5 SYN / Sekunde noch Ok.

SNMP: Ergänzung der Statuswerte aus den Infos von /proc/net/dev

Verbesserung für IPv6 Bridging

SCEP: Wenn der CA Identity Parameter für die URL unerlaubte Zeichen enthält wird der Wert URL-Encoded gesetzt.

Anzeige zusätzlicher Warnungen im MCCConfig (ab Vers.: 2_0_3_9) in der Spalte „Status“:

- Für Zertifikate die zeitnah ablaufen oder schon abgelaufen sind
- Für fehlerhaft konfigurierten Ping-Test.

Nach einem „Reset to defaults“ der Config über das Webinterface oder auch beim Upload einer Konfiguration wechselt die Ansicht automatisch nach 2 Sekunden zur Konfigurations-Webseite.

Bugfixes:

das AuxIn wird beim MC2LX8 jetzt richtig verarbeitet

Die USB-Spannung wird jetzt früher eingeschaltet, sodass ein aufgesteckter USB-Speicher frühzeitig erkannt werden kann. Damit funktioniert jetzt auch die Config-Stick Erkennung zuverlässig.

Korrektur beim Upload einer Konfiguration über das Webinterface:
Die Passwörter werden jetzt richtig verarbeitet

Firmware 3.14m → 3.14n (25.07.2023)

Sicherheits-Updates:

Wechsel der Linux Kernel Version von 6.1.33 → 6.1.36

Funktionelle Änderungen:

- 1) Webserver-Security:
 - Es können jetzt Vorgaben für die TLS session's handshake Algorithmen gemacht werden.
 - Neue Option Send HSTS Header
- 2) EAP: EAP-TTLS kann jetzt auch ohne Zertifikate durchgeführt werden. (ähnlich wie bei EAP-PEAP)
- 3) wpa_supplicant: jetzt mit 802.11v Support.
- 4) Wireless: Anzeige in der AP-Liste ob ein Accesspoint 802.11v unterstützt.
- 5) Seriell: Die serielle Schnittstelle kann jetzt auch per TLS kommunizieren.
Dazu können auch Zertifikate zur Authentifizierung installiert werden
- 6) Bridge/NAT: Warnung vor Konflikten von lokalen Services des Geräts mit per Config definierter NAT-Regeln.
- 7) MQTT-Bridge: Jetzt auch mit lokalem Websocket-Port (Default 8080)

Firmware 3.14k → 3.14m (14.06.2023)

Sicherheits-Updates:

Wechsel der Linux Kernel Version von 6.1.23 → 6.1.33

Funktionelle Änderungen:

1. wpa_supplicant aktualisiert auf 2.11-dev (Git Rev. 95C3f0d1)
2. Verbesserung bei der Relais-Steuerung über die REST-API:
Fehlerhafte Sequenzen und Relais-Befehle werden jetzt mit HTTP Error 400 abgelehnt.
3. Ausgabe einer Warnung im Debuglog, wenn bei der Score-Berechnung alle passenden SSID's mit 0 bewertet werden. Das deutet darauf hin, dass eine der Crypto-Einstellungen nicht passt.
4. Warnung im Debuglog nach dem Start wenn Zertifikate (Client und CA-Zertifikate) geladen sind, die bald ablaufen oder schon abgelaufen sind.

Firmware 3.14i → 3.14k (16.05.2023)

Funktionelle Änderungen:

1. Das Relais ist jetzt auch über die REST-API und mit Hilfe von Anweisungssequenzen steuerbar.

2. Authentifizierung von einzelnen API/URLs:
Dadurch ist es möglich, Zugriffe auf bestimmte API-Funktionen mit einem separaten User/Passwort abzusichern ohne das User/Passwort für die Gerätekonfiguration verwenden zu müssen.
3. 5G/LTE: Firmware Update support für RM520N-GL

Bugfix:

- Segfault-Fehler in der MQTT Funktion behoben (TLS-Write)
- Segfault-Fehler im Timermodul behoben (Blacklist + ConfigChange)