RELEASE NOTES

LCOS LX
7.20 Rel

Inhaltsübersicht

02 **1. Einleitung**

02 **2. Das Release-Tag in der Software-Bezeichnung**

03 **3. Gerätespezifische Kompatibilität zu LCOS LX**

03 **4. Hinweise zu LCOS LX**
03 Informationen zu Werkseinstellungen

03 **5. Bekannte Einschränkungen**

04 **6. Historie LCOS LX**
04 LCOS LX - Änderungen 7.20.0087 Rel

08 **7. Allgemeine Hinweise**
08 Haftungsausschluss
08 Sichern der aktuellen Konfiguration

ROHDE&SCHWARZ
Make ideas real

1. Einleitung

Alle Mitglieder der LCOS Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte R&S®LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle R&S®LANCOM Produkte verfügbar und wird von Rohde & Schwarz Networks and Cybersecurity kostenlos zum Download angeboten.

Rohde & Schwarz Networks and Cybersecurity hält in einer LCOS-Firmware verwendete Programmbibliotheken auf dem aktuellen Sicherheitsstand und behebt Sicherheitslücken auch dann, wenn sie in der Firmware nicht ausnutzbar sind.

Dieses Dokument beschreibt die Neuerungen der LCOS LX Software Release 7.20 Rel.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 7 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS LX-Version finden Sie im Support-Bereich unserer Webseite.

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von Rohde & Schwarz Networks and Cybersecurity getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger Betriebssystem-Versionen und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS LX

Grundsätzlich werden alle R&S®LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten. Auch für Geräte, die keine aktuelle LCOS LX-Version unterstützen, werden in regelmäßigen Abständen LCOS LX Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstützte LCOS LX-Version für Ihr Gerät finden Sie unter Lifecycle-Richtlinien.

4. Hinweise zu LCOS LX

Informationen zu Werkseinstellungen

Geräte, die mit LCOS LX ausgeliefert werden, kontaktieren automatisch die R&S®LANCOM Management Cloud (R&S®LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme neuer Geräte. Falls die R&S®LMC nicht verwendet werden soll, kann diese Funktionalität im LANconfig jederzeit unter ‚Management > LMC' deaktiviert werden. Eine spätere Verwendung der R&S®LMC ist jederzeit wieder manuell aktivierbar.

5. Bekannte Einschränkungen

- Lokale Konfigurationsänderungen werden nicht in die R&S®LMC übertragen.
- Das Skripting des Gerätes aus der R&S®LMC wird aktuell noch nicht unterstützt, jedoch die Verwendung von Add-Ins.

6. Historie LCOS LX

LCOS LX - Änderungen 7.20.0087 Rel

Für den WLC-verwalteten Betrieb eines Access Points mit LCOS LX 7.20 ist auf dem R&S®LANCOM WLC mindestens die LCOS-Version 10.94 erforderlich.

Neue Features

Allgemein

- Die Einschränkungen beim Betrieb des R&S®LANCOM LX-7400 mit PoE 802.3at wurden angepasst:
  - die Ethernet-Geschwindigkeit von ETH1 wird auf 1 GBit/s gedeckelt
  - USB kann nicht verwendet werden
  - die 6 GHz WLAN-Streams werden von 4x4 auf 2x2 reduziert

  Weitere Einschränkungen finden nicht statt.
- Wurden in der Vergangenheit ein Hauptgerätepasswort oder Nutzer-Passwörter manuell mit den veralteten Hash-Verfahren MD5 oder DES angelegt, können diese ab LCOS LX 7.20 nicht mehr verwendet werden. Setzen Sie in diesem Fall **vor dem Update** die Passwörter neu, z.B. mittels LANconfig oder dem ‚passwd'-Kommando. Als Hashverfahren kommt dabei SHA256 zum Einsatz.

  Info: Eine Verwendung dieser veralteten Hashverfahren war nur auf expliziten Nutzerwunsch möglich, standardmäßig kommt in allen LCOS LX-Versionen das Verfahren SHA256 zum Einsatz.
- Zusätzliche Administratoren und separate Benutzerrechte sind nun konfigurierbar.
- Unterstützung für Public-Key-Authentifizierung in SSH
- Unterstützung für Cron-Jobs zur Zeitplanung von Aktionen

WLAN

- Unterstützung für den WLAN End-to-End-Test zur Beurteilung der Funktionsfähigkeit von WLAN-Netzen durch Simulation eines WLAN-Clients
- Überarbeitung des Client-Managements zur Verteilung von Clients via 802.11k/v
- Unterstützung einer Firewall zum Filtern von Datenverkehr von und zu WLAN-Netzwerken auf IP-Ebene, inkl. DNS-Unterstützung
- Aktualisierung des WLAN-Treibers für erhöhte Stabilität und Kompatibilität

Korrekturen / Anpassungen

- Fehlerbehebung für CVE-2026-98432
- Bei Verwendung eines Access Points mit LCOS LX ab Version 7.12 an einem WLAN-Controller mit LCOS 10.94 und konfigurierter Sendeleistungsreduktion wurde die Reduktion nicht übernommen – der Access Point sendete weiterhin mit voller Leistung.
- Die PoE-Aushandlung per LLDP dauert einige Zeit. Dadurch startete der WLAN-Dienst, bevor die PoE-Aushandlung per LLDP erfolgte. Wenn Access Points der Modelle LW-700, LX-7200 und LX-7400 via PoE an einem Switch betrieben wurden, der vor der PoE-Aushandlung per LLDP nur 802.3af mit 15,4 W lieferte, führte dies dazu, dass die Funkmodule der Access Points nach einem Neustart nicht mehr starteten. Der Status der Module verblieb dabei auf ‚Modul inaktiv'.

- Wenn auf einem Access Point ein tagged Management VLAN konfiguriert und am Switch-Port die Authentifizierungsmethode ‚802.1X Multi Auth' eingestellt war, schlug die 802.1X-Authentifizierung fehl.
- In einem WLAN-Controller-Szenario melden die Access Points neu verbundene Clients an den WLAN-Controller (add station event). Bei diesen Meldungen waren die Interfaces vertauscht. Dies führte dazu, dass weder die korrekte Gesamt-Anzahl der verbundenen Clients an den WLAN-Controller gemeldet wurde (Status/WLAN-Management/Client-Count auf dem WLAN-Controller), noch die Anzahl an Clients je WLAN-Interface (Status/WLAN-Management/AP-Status/Active-Radios auf dem WLAN-Controller).
- In den Status-Tabellen ‚Station-Table', ‚IAPP-Table' und ‚Interfaces' (alle im Konsolen-Pfad ‚Status/WLAN') konnte keine leere SSID eingetragen werden. Dies führte bei Verwendung einer versteckten SSID (Closed-Network) dazu, dass diese nicht in den genannten Tabellen hinterlegt werden konnte. In der ‚Station-Table' waren dadurch auch keine Einträge für die mit der versteckten SSID verbundenen Clients enthalten.
- Die DHCPv6 IAID (Identity Association Identifier) in DHCPv6-Requests wurde zufällig generiert, statt diese statisch zu erzeugen.
- Die DHCPv6 IAID wird jetzt basierend auf der Interface-MAC-Adresse erzeugt.
- Der DHCPv6-Client sendete in sehr kurzen Intervallen DHCPv6-Solicit-Pakete, wenn kein DHCPv6-Server antwortete.
  Der Timer zum Senden der DHCPv6-Solicit-Pakete steigt jetzt an.
- Bei Verwendung eines WLC-Tunnels mit einem VLAN konnte einem WLAN-Client kein abweichendes VLAN per Dynamic VLAN zugewiesen werden. Dies führte dazu, dass der Client Zugriff auf das falsche Netzwerk erhielt.
- Bei einem DHCP-Renew wurden geänderte DNS-Server nicht übernommen.
- Bei der Stromversorgung eines LX-7500 per Dual-PoE konnte es bei einigen 802.3at-fähigen Switches vorkommen, dass der Access Point nach einem Neustart auf dem zweiten Ethernet-Port keine 25,5 W mehr anfragte und dadurch nur 13 W zugewiesen bekam. Dies führte dazu, dass die Funktionalität des Access Points eingeschränkt war und das WLAN nicht ausgestrahlt wurde.
- Wenn die Hotspot-Tabelle im Access Point mehr als 512 Einträge enthielt, war kein Zugriff mehr per Webinterface möglich und Konfigurations-Rollouts per LMC schlugen ebenfalls fehl.
- War bereits ein ‚Managed Address Configuration Flag' (M-Flag) im IPv6 Router Advertisement vorhanden, ignorierte der Access Point ein gegebenenfalls vorhandenes ‚Autonomous Address Configuration Flag' (A-Flag). Dies führte dazu, dass der Access Point zwar eine IPv6-Adresse per DHCPv6 beziehen, aber keine eigene IPv6-Adresse per SLAAC für die Präfixe generieren konnte.
- Wenn in einem WLAN-Controller-Szenario ein Land eingestellt wurde, welches der Access Point nicht unterstützt, stellte dieser als Land Europa ein, statt die Änderung abzulehnen.
  Ein Access Point mit nicht vorhandenem WLAN-Profil sendet jetzt bei einer ungültigen Länder-Einstellung eine entsprechende Fehlermeldung an den WLAN-Controller und das WLAN wird nicht ausgestrahlt.
  Ein Access Point mit bereits vorhandenem WLAN-Profil samt gültiger Länder-Einstellung sendet bei einer Änderung in ein ungültiges Land ebenfalls eine Fehlermeldung an den WLAN-Controller. Das WLAN wird weiterhin mit der bisherigen gültigen Länder-Einstellung ausgestrahlt.
- Die ‚Client-Isolation' unterstützt jetzt auch IPv6 und kann damit nicht mehr nur für IPv4 verwendet werden. Gateways werden allerdings noch nicht anhand der Router-Advertisements und DHCPv6-Antworten automatisch erkannt und müssen daher manuell eingetragen werden.
- Auf dem R&S®LANCOM LW-600 war das Paket-Capturing im Raw-Modus aufgrund der Hardwareaussattung nicht funktional und wurde daher entfernt.

- Wenn auf einem Access Point ein tagged Management VLAN konfiguriert und am Switch-Port die Authentifizierungsmethode ‚802.1X Multi Auth' eingestellt war, schlug die 802.1X-Authentifizierung fehl.
- In einem WLAN-Controller-Szenario melden die Access Points neu verbundene Clients an den WLAN-Controller (add station event). Bei diesen Meldungen waren die Interfaces vertauscht. Dies führte dazu, dass weder die korrekte Gesamt-Anzahl der verbundenen Clients an den WLAN-Controller gemeldet wurde (Status/WLAN-Management/Client-Count auf dem WLAN-Controller), noch die Anzahl an Clients je WLAN-Interface (Status/WLAN-Management/AP-Status/Active-Radios auf dem WLAN-Controller).
- In den Status-Tabellen ‚Station-Table', ‚IAPP-Table' und ‚Interfaces' (alle im Konsolen-Pfad ‚Status/WLAN') konnte keine leere SSID eingetragen werden. Dies führte bei Verwendung einer versteckten SSID (Closed-Network) dazu, dass diese nicht in den genannten Tabellen hinterlegt werden konnte. In der ‚Station-Table' waren dadurch auch keine Einträge für die mit der versteckten SSID verbundenen Clients enthalten.
- Die DHCPv6 IAID (Identity Association Identifier) in DHCPv6-Requests wurde zufällig generiert, statt diese statisch zu erzeugen.
- Die DHCPv6 IAID wird jetzt basierend auf der Interface-MAC-Adresse erzeugt.
- Der DHCPv6-Client sendete in sehr kurzen Intervallen DHCPv6-Solicit-Pakete, wenn kein DHCPv6-Server antwortete.
  Der Timer zum Senden der DHCPv6-Solicit-Pakete steigt jetzt an.
- Bei Verwendung eines WLC-Tunnels mit einem VLAN konnte einem WLAN-Client kein abweichendes VLAN per Dynamic VLAN zugewiesen werden. Dies führte dazu, dass der Client Zugriff auf das falsche Netzwerk erhielt.
- Bei einem DHCP-Renew wurden geänderte DNS-Server nicht übernommen.
- Bei der Stromversorgung eines LX-7500 per Dual-PoE konnte es bei einigen 802.3at-fähigen Switches vorkommen, dass der Access Point nach einem Neustart auf dem zweiten Ethernet-Port keine 25,5 W mehr anfragte und dadurch nur 13 W zugewiesen bekam. Dies führte dazu, dass die Funktionalität des Access Points eingeschränkt war und das WLAN nicht ausgestrahlt wurde.
- Wenn die Hotspot-Tabelle im Access Point mehr als 512 Einträge enthielt, war kein Zugriff mehr per Webinterface möglich und Konfigurations-Rollouts per LMC schlugen ebenfalls fehl.
- War bereits ein ‚Managed Address Configuration Flag' (M-Flag) im IPv6 Router Advertisement vorhanden, ignorierte der Access Point ein gegebenenfalls vorhandenes ‚Autonomous Address Configuration Flag' (A-Flag). Dies führte dazu, dass der Access Point zwar eine IPv6-Adresse per DHCPv6 beziehen, aber keine eigene IPv6-Adresse per SLAAC für die Präfixe generieren konnte.
- Wenn in einem WLAN-Controller-Szenario ein Land eingestellt wurde, welches der Access Point nicht unterstützt, stellte dieser als Land Europa ein, statt die Änderung abzulehnen.
  Ein Access Point mit nicht vorhandenem WLAN-Profil sendet jetzt bei einer ungültigen Länder-Einstellung eine entsprechende Fehlermeldung an den WLAN-Controller und das WLAN wird nicht ausgestrahlt.
  Ein Access Point mit bereits vorhandenem WLAN-Profil samt gültiger Länder-Einstellung sendet bei einer Änderung in ein ungültiges Land ebenfalls eine Fehlermeldung an den WLAN-Controller. Das WLAN wird weiterhin mit der bisherigen gültigen Länder-Einstellung ausgestrahlt.
- Die ‚Client-Isolation' unterstützt jetzt auch IPv6 und kann damit nicht mehr nur für IPv4 verwendet werden. Gateways werden allerdings noch nicht anhand der Router-Advertisements und DHCPv6-Antworten automatisch erkannt und müssen daher manuell eingetragen werden.

- Auf dem R&S®LANCOM LW-600 war das Paket-Capturing im Raw-Modus aufgrund der Hardwareaussattung nicht funktional und wurde daher entfernt.
- Die veralteten WLAN-Verschlüsselungsverfahren WEP und WPA(1/2)-TKIP werden automatisch zur Laufzeit auf WPA2-CCMP adaptiert. Die Konfigurationsmöglichkeiten für WEP und WPA(1/2)-TKIP werden in einer zukünftigen LCOS LX-Version entfernt.

7. Allgemeine Hinweise

Haftungsausschluss

Die Rohde & Schwarz Networks and Cybersecurity übernimmt keine Gewähr und Haftung für nicht von der Rohde & Schwarz Networks and Cybersecurity entwickelte, hergestellte oder unter dem Namen der Rohde & Schwarz Networks and Cybersecurity vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Sichern der aktuellen Konfiguration

Bitte sichern Sie vor dem Update Ihrer R&S®LANCOM Geräte auf eine neue LCOS LX-Version unbedingt Ihre Konfigurationsdateien!

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf eine ältere Firmware **nicht mehr automatisch möglich.**

Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch Rohde & Schwarz Networks and Cybersecurity ausgeschlossen werden können.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u.a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen. 11/2026

ROHDE&SCHWARZ
Make ideas real