RELEASE NOTES

LCOS LX
7.12 RU2

Inhaltsübersicht

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.

Dieses Dokument beschreibt die Neuerungen der LCOS LX Software Release 7.12 RU2.

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 7.12.0098 RU2

Korrekturen / Anpassungen

- 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.

LCOS LX - Änderungen 7.12.0097 RU1

Korrekturen / Anpassungen

- In der glib-Programmbibliothek wurden durch ein Update Sicherheitslücken behoben, die in folgenden CVEs beschrieben werden: [1]
  - CVE-2025-6052
  - CVE-2024-34397
  - CVE-2024-52533
  - CVE-2025-4056
- In der libxml2-Programmbibliothek wurden durch ein Update Sicherheitslücken behoben, die in folgenden CVEs beschrieben werden: [1]
  - CVE-2025-32414
  - CVE-2025-32415
- Es wurde eine Sicherheitslücke im Message Bus ‚ubusd' behoben, welche im CVE-2025-62526 beschrieben ist. [1]
- Der Wert für die Sendeleistung (EIRP) konnte 3-stellig angegeben werden.
- Der TFTP-Server hörte lediglich auf IPv4-Adressen. In der Folge ließ sich die Sysinfo nicht per IPv6 auslesen und Geräte mit IPv6-Adresse konnten nicht im LANconfig gefunden werden.
- Wenn in der Kommandozeile eines Access Points der Befehl ‚ls /Status/Bridge/VLAN-Table/' oder im Pfad ‚Status/Bridge/VLAN-Table/' der Befehl
  ‚ls' eingegeben wurde, kam es zu einem unvermittelten Neustart des Gerätes.
- Wenn per Kommandozeile Änderungen an der Tabelle ‚Setup/Bridge/DHCP-Snooping' durchgeführt wurden, die einen Platzhalter zum Beschreiben mehrerer Spalten im Befehl enthielten (z.B. ‚set NETWORK %i'), kam es zu einem unvermittelten Neustart des Access Points.
- Wurde im Konsolen-Pfad ‚Setup/WLAN/WDS/Encryption' für die ‚WPA2-3-Session-Keytypes' eine Bitmaske mit dem Wert 4 oder höher gesetzt, führte dies zu einem unvermittelten Neustart des Access Points.
- Wurde ein R&S®LANCOM LX-7200 / LX-7200E im PoE-Modus 802.3af betrieben, zeigte der Access Point im Konsolen-Pfad ‚Status/Hardware/Power' als Power-Status fälschlicherweise „Fully Operational" an, obwohl die Funktionalität eingeschränkt war. Weiterhin wurde im Pfad ‚Status/Hardware/Power/Ports' der Port ETH2 als ‚DC' bezeichnet.
- Ein Wechsel in einen Tabellen-Eintrag mit dem Konsolen-Befehl ‚cd' war nicht möglich, wenn der Index das Zeichen ‚-' enthielt oder der Index nicht an erster Stelle in dem Eintrag stand.
- Der interne Name der Paketfilter-Regeln für die Client-Isolierung darf maximal 31 Zeichen lang sein. Wenn der konfigurierte Name für das WLAN-Netzwerk zu lang war, wurde dieses Limit überschritten und die Paketfilter-Regel konnte nicht geschrieben werden. Dadurch konnte das hinterlegte Ziel nicht von den isolierten WLAN-Clients erreicht werden.

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

LCOS LX - Änderungen 7.12.0042 Rel

Neue Features

- DHCP-Option 82: DHCPv4 Circuit-ID und Remote-ID kann in DHCP-Requests eingefügt werden
- mDNS-Filter
- Cloud-based Hotspot: Walled-Garden-Hosts (freie Hosts/Netze) können konfiguriert werden
- Cloud-based Hotspot: Ziele in RFC1918-Netzen können selektiv freigeschaltet werden

Korrekturen / Anpassungen

- Bei aktivem MLO funktionierte der ARC-Scan auf Access Points mit Wi-Fi 7- Unterstützung (R&S®LANCOM LW-700, LX-7200, LX-7300, LX-7400 und LX-7500) nicht. Weiterhin wurde nach Ausführen des ARC-Scans kein WLAN mehr ausgestrahlt.
- Fiel ein angeschlossener USB-Dongle aus, war auch nach Aus- und Einschalten der Stromversorgung für den USB-Port keine Kommunikation mit dem USB-Dongle möglich.
- Access Points mit externen WLAN-Antennen interpretierten den vom WLAN Controller übermittelten Wert für den Standard-Antennen-Gewinn als 0, anstatt den Standard-Antennen-Gewinn der mitgelieferten Stab-Antennen zu verwenden.
- In seltenen Fällen leuchtete die Power-LED des Access Points gelb statt grün, wenn die PoE-Aushandlung per LLDP erfolgte. Dabei handelte es sich um einen reinen Anzeigefehler. Die Performance wurde dadurch nicht beeinträchtigt.
- Eine konfigurierte Bandbreitenlimitierung (Client-Rx/Tx-Limit) wurde nicht angewendet, wenn in dem Szenario mit statischem VLAN gearbeitet wurde.
- Empfing der Access Point bei Verwendung des LMC-Hotspot mit statischen VLANs ein zu großes Paket, welches fragmentiert werden musste, wurde nur das erste Fragment übertragen und weitere Fragmente verworfen. Dies führte dazu, dass die Kommunikation nur stark eingeschränkt funktionierte.
- Bei den Access Points R&S®LANCOM LX-7300 und LX-7500 funktionierte die LLDP-Aushandlung für PoE mit Switches des Herstellers HPE Aruba nicht korrekt. In der Folge erhielten die Access Points zu wenig Strom vom Switch und strahlten keine SSID(s) aus.
- Die Programmbibliotheken libpcap, apr (Apache Portable Runtime) und libxml2 wurden aktualisiert, um Sicherheitslücken zu schließen, welche in den folgenden CVE-Meldungen beschrieben sind:
  - libpcap: CVE-2023-7256, CVE-2024-8006
  - apr: CVE-2022-24963, CVE-2022-28331, CVE-2021-35940
  - libxml2: CVE-2024-25062
- Eine im WLAN Controller konfigurierte Sendeleistungsreduktion war nur aktiv, wenn der Antennengewinn-Modus ‚Benutzerdefiniert' eingestellt war. Die Sendeleistungsreduktion ist nun unabhängig vom eingestellten Antennengewinn-Modus aktiv.

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