Release Notes

LCOS LX

5.36 RU4

Inhaltsübersicht

1. Einleitung

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

Dieses Dokument beschreibt die Neuerungen der LCOS LX Software Release 5.36 RU4.

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 https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)

Ein Release Candidate ist umfangreich von LANCOM 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 LANCOM Betriebssystem-Versionen. Wird für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)

Dient zur nachträglichen Weiterentwicklung einer initialen Release-Version und enthält Detailverbesserungen, Bug Fixes und kleinere Features.

Security Update (SU)

Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard.

3. Gerätespezifische Kompatibilität zu LCOS LX

Grundsätzlich werden alle 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 unterstütze LCOS LX-Version für Ihr Gerät finden Sie unter https://www.lancom-systems.de/produkte/firmware/lifecycle-management/produkttabellen-lcos-lifecycle-management

4. Hinweise zu LCOS LX

Informationen zu Werkseinstellungen

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

5. Historie LCOS LX

LCOS LX-Änderungen 5.36.0154 RU4

Korrekturen / Anpassungen

→ Nach dem Ausführen des Konsolen-Befehls ‚beginscript' wurden bestimmte danach ausgeführte Befehle (etwa ‚ping') mit der Meldung „Finished script successfully" oder „Finished script with error (invalid command)" quittiert.

→ WLAN-Clients wurden nach Ablauf des RADIUS Session-Timeouts aus dem WLAN abgemeldet, statt eine neue 802.1X-Authentifizierung durchzuführen.

→ Wenn die CAPWAP-Verbindung zu einem LANCOM WLAN Controller abbrach, wurden alle verbundenen WLAN-Clients nach dem Wiederaufbau der Verbindung vom WLAN-Netzwerk getrennt.

→ Mit dem Konsolen-Befehl ‚startlmc' kann ein Pairing mit der LMC auch von pre-claimed Geräten vorgenommen werden. Bei Ausführung des Befehls ‚startlmc' in LCOS LX wurde fälschlicherweise zusätzlich noch verpflichtend ein Aktivierungscode aus der LMC angefordert.

→ Wenn ein LANCOM LW-500 IPv4- bzw. IPv6-Pakete mit unvollständigem Header empfing, konnte dies dazu führen, dass der Access Point nicht mehr erreicht werden konnte.
Zur Behebung dieses Verhaltens wurde im Pfad ‚Setup/LAN' die Option ‚Hardware-Flow-Dispatching' eingebaut. Standardmäßig ist diese Option im Status ‚Yes', sodass der Datenverkehr auf alle Prozessorkerne des Gerätes aufgeteilt wird. Sollte es zu dem beschriebenen Verhalten kommen, muss die Option per Kommandozeile inaktiv geschaltet werden.
Verwenden Sie dazu den Befehl „set Setup/LAN/Hardware-Flow-Dispatching No", gefolgt von dem Befehl „flash yes" (zum peristenten Speichern der Einstellung).

LCOS LX-Änderungen 5.36.0137 RU3

Korrekturen / Anpassungen

→ Die ‚DHCP lease time' des Cloud-managed Hotspots wurde von 24 Stunden auf 8 Stunden verringert.

→ In Szenarien mit 802.1X-Authentifizierung und gleichzeitiger Verwendung von FT (Fast Transition) wird nun pro Station und BSSID ein PMK zwischengespeichert.

→ Bei der initialen WLAN-Anmeldung eines Clients in einem 802.1X-Szenario mit Verwendung von FT (Fast Transition) wurde der PMK (Pairwise Master Key) nur für das WLAN-Interface auf dem aktuell verwendeten Frequenzband erstellt, nicht aber für WLAN-interfaces mit der gleichen SSID auf einem anderen Frequenzband. Wenn sich der WLAN-Client zu einem späteren Zeitpunkt mit der SSID auf einem anderen Frequenzband verbinden wollte, führte dies dazu, dass die Anmeldung entweder fehlschlug (bei Verwendung von FT) oder die komplette Schlüssel-Aushandlung erneut durchlaufen werden musste.

→ Wenn eine Änderung der Kanäle für eine SSID vorgenommen wurde, welche der Access Point bereits ausstrahlte, wurden die geänderten Kanäle nicht verwendet.

→ Es war nicht möglich, über den Menüpunkt ‚RADIUS-Profile bearbeiten' die Verschlüsselungsprofile für WPA2-802.1X zu bearbeiten. Hier wurde anstatt der auswählbaren Daten ein leeres Fenster angezeigt. Weiterhin konnte auch der Zeitrahmen im Menü ‚WLAN-Konfiguration - SSID' nicht bearbeitet werden.

→ War kein Gateway hinterlegt (per DHCP gelernt), gab es keine Route für Multicast-Pakete. Dies führte dazu, dass IAPP-Pakete nicht übertragen werden konnten und dadurch Roaming nicht unterbrechungsfrei funktionierte.

→ Aufgrund eines Fehlers in der Behandlung von Pairwise Master Keys (PMKs) kam es bei LCOS LX-Access Points zu Speichermangel. In der Folge startete ein Access Point unvermittelt neu.

→ Der von einem WLAN-Client übermittelte Benutzername konnte in der WLAN-Stationstabelle mit maximal 32 Zeichen eingetragen werden. Es sind nun Namen mit bis zu 64 Zeichen möglich.

→ Ein Fehlverhalten in der Bridge führte dazu, dass ein Access Point ein selbst versendetes IP-Paket wieder empfing. Dies führte dazu, dass der Access Point nicht mehr erreicht werden konnte und z.B. die Verbindung zu einem WLAN-Controller verlor.

→ Es war nicht möglich, im WEBconfig eine LMC-Domäne einzutragen, die eine Zahl enthielt (z.B. lmc.test1.de).

→ Wenn im AP-Profil eines WLC eine Basis-Geschwindigkeit konfiguriert war, wurde unabhängig vom konfigurierten Wert immer eine Geschwindigkeit von 1 MBit/s verwendet.

→ In der Konfiguration eines Access Point blieb ein vom WLC übermitteltes Netzwerkprofil leer, wenn das konfigurierte WLAN-Passwort ein Leerzeichen enthielt.

→ In einem WLC-Szenario wurde der PMK eines WLAN-Clients erst nach ca. 25 Sekunden an den WLC übermittelt. In der Folge kam es zu Problemen beim Roaming.

→ Konnte der CAPWAP-Dienst eines Access Points die vom WLAN-Controller übermittelte Konfiguration nicht interpretieren (etwa aufgrund eines fehlerhaften Parameters), meldete der Access Point dies nicht an den WLAN-Controller. Dies führte dazu, dass der WLAN-Controller die Konfiguration bis zum Ablauf eines Timeouts immer wieder an den Access Point sendete.
Der CAPWAP-Dienst sendet jetzt bei einem Fehler direkt eine Fehlermeldung an den WLAN-Controller.

→ Der CAPWAP-Dienst in einem Access Point konnte ein von einem WLAN-Controller empfangenes ‚Update Request' mit leerem ‚WTP Name' nicht verarbeiten. Dies führte dazu, dass der Access Point nicht mehr verwaltet werden konnte.

→ Bei Verwendung eines ‚Untagged-VLAN' wurden innerhalb dieses VLANs auch Pakete aus dem VLAN 1 (INTRANET) übertragen.

LCOS LX-Änderungen 5.36.0129 SU2

Korrekturen / Anpassungen

→ Sicherheitsverbesserungen durch ein Update der OpenSSL-Version auf 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 und CVE-2022-4450)

LCOS LX-Änderungen 5.36.0103 SU1

Korrekturen / Anpassungen

→ Behebung von CVE-2022-24810, CVE-2022-24809, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806 und CVE-2022-24805.

LCOS LX-Änderungen 5.36.0069 Rel

Korrekturen / Anpassungen

→ Es wurde eine Schwachstelle in der zlib-Bibliothek behoben (CVE-2018-25032).

→ Es wurde eine Schwachstelle in der OpenSSL-Bibliothek behoben (CVE-2022-0778).

→ Wenn sich ein Access Point mit einem LANCOM WLAN-Controller verbinden wollte, der in einem entfernten Netzwerk betrieben wurde, konnte die Verbindung sporadisch fehlschlagen, da der WLAN-Controller die Verbindungsanfrage aufgrund eines dem LCOS unbekannten Parameters im verwendeten DTLS-Protokoll verwarf.

→ Wenn ein LANCOM WLAN-Controller bei einem verwalteten LANCOM LW-500 die Funktion ‚Multicast-zu-Unicast' aktivieren wollte, schlug dies fehl, weil der LANCOM LW-500 nicht das richtige Multicast-Protokoll verwendete.

→ Bei Verwendung der Fast Roaming-Funktion konnte es aufgrund eines Speicherlecks sporadisch zu unvermittelten Neustarts der Access Points kommen.

→ Ein Access Point verfügt über unterschiedliche MAC-Adressen für die beiden WLAN-Schnittstellen. In einem WLAN-Controller-Szenario meldeten die Access Points beim Hinzufügen und Löschen von WLAN-Endgeräten jeweils die MAC-Adresse einer anderen WLAN-Schnittstelle (WTP MAC) an den WLAN-Controller, sodass diese nicht übereinstimmten. Dadurch kam es auf dem WLAN-Controller und den Access Points zu einer Diskrepanz der angemeldeten WLAN-Endgeräte in der Stationstabelle.
→ Bei einem Verbindungsversuch per LL2M mit Angabe der korrekten Schnittstelle konnte es vorkommen, dass die Angabe der Schnittstelle nicht erkannt wurde und stattdessen die für LL2M verfügbaren Optionen ausgegeben wurden. Der Verbindungsaufbau per LL2M schlug dadurch fehl.
→ Wenn im LANCOM WLAN-Controller nur eine Änderung der Netzmaske im IP-Parameter-Profil durchgeführt wurde, übertrug der WLC diese Änderung an den Access Point. Dieser hatte die Änderung aufgrund einer fehlenden Vergleichsfunktion (Ist-Zustand/Soll-Zustand) nicht übernommen und verwendete weiterhin die alte Netzmaske.
→ Es konnte sporadisch zu Paket-Verlusten innerhalb eines WLC-Tunnels kommen.

LCOS LX-Änderungen 5.36.0047 RC1

Neue Features

→ Unterstützung des LL2M-Protokolls
→ Unterstützung für Proxy-ARP / ARP-Handling im WLAN
→ Untagged-VLAN-/Access-Port-Konfiguration weiterer Ethernet-Ports an Access Points

Korrekturen / Anpassungen

→ RADIUS-Access-Requests im Rahmen einer MAC-Adress-Prüfung werden nun mit dem RADIUS-Service-Typ ‚Framed' sowie mit den Attributen NAS-Port und NAS-Port-Id versehen.
→ In einem WLAN-Controller-Szenario konnte es bei Nutzung eines Zeitrahmens für das verwendete WLAN-Profil nach Deaktivierung und anschließender Aktivierung des WLAN-Profils durch den Zeitrahmen vorkommen, dass die SSID nicht korrekt mit der Bridge verknüpft war. Dadurch konnten WLAN-Endgeräte keine IP-Adresse per DHCP beziehen und nicht über diesen Access Point kommunizieren.

→ Befinden sich ein WLAN-Controller und ein Access Point in unterschiedlichen Netzwerken, versucht der Access Point den WLAN-Controller über den DNS-Namen ‚WLC-Address' zu erreichen. War in der Konfiguration des Access Points bereits ein DNS-Suffix hinterlegt und wurde das DNS-Suffix vom WLAN-Controller ebenfalls verteilt, führte dies dazu, dass das DNS-Suffix zweimal an ‚WLC-Address' angehängt wurde. Dadurch konnte der Access Point die IP-Adresse des WLAN-Controllers nicht mehr auflösen und es war keine Kommunikation mehr zwischen den Geräten möglich.

→ Ein Access Point versucht einen WLAN-Controller über den DNS-Namen ‚WLC-Address' zu erreichen, wenn sich dieser in einem anderen Netzwerk befindet. Ein vom WLAN-Controller zugewiesenes DNS-Suffix wurde jedoch nicht bootpersistent gespeichert und stand somit nach einem Neustart nicht mehr zu Verfügung. Dies führte dazu, dass der Access Point den WLAN-Controller nicht mehr erreichen konnte, wenn der DNS-Server lediglich ‚WLC-Address.DNS-Suffix' auflöste.

→ Auf der Kommandozeile können gefundene BLE-Beacons mit dem Befehl ‚ls st/lbs/ble' aufgelistet werden. Es konnte jedoch vorkommen, dass in dieser Liste keine BLE-Beacons angezeigt wurden, obwohl welche in der Umgebung des Access Points vorhanden waren.

→ In der WEBconfig wurden Verbesserungen bei der Funktion und Anzeige eines BLE-Scans durchgeführt.

→ Bei den LANCOM LCOS LX-Access Points konnte es aufgrund von Speicherverlusten vorkommen, dass die Geräte ‚einfroren' und ihren Dienst einstellten. Ein Neustart der Geräte behob das Verhalten bis zum nächsten Speicherverlust. Dieses Verhalten trat vermehrt bei den Geräten der LANCOM LW-Serie auf (LW-500 & LW-600).

6. Bekannte Einschränkungen

→ Bei Verwendung beider LAN-Ports zur Durchleitung des Datenverkehrs wird nur ungetaggter Datenverkehr oder Datenverkehr mit dem für den Managementzugriff verwendeten VLAN-Tag durchgeleitet.
→ Lokale Konfigurationsänderungen werden nicht in die LMC übertragen.
→ Das Skripting des Gerätes aus der LMC wird aktuell noch nicht unterstützt, jedoch die Verwendung von Add-Ins.

7. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Sichern der aktuellen Konfiguration

Bitte sichern Sie vor dem Update Ihrer 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 LANCOM Systems ausgeschlossen werden können.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de