Release Notes

LCOS
10.94 RU3

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 Software Release 10.94 RU3 sowie die Änderungen und Verbesserungen zur Vorversion.

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

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite www.lancom.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 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 LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS 10.94

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-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstütze LCOS-Version für Ihr Gerät finden Sie unter
www.lancom.de/produkte/firmware/software-lifecycle-management

LANCOM Geräte ohne Unterstützung ab LCOS 10.94

→ 1790-4G
→ 1790VA-4G
→ 1793VA-4G
→ ISG-1000
→ ISG-4000
→ 883 VoIP
→ 730VA
→ L-321agn (R2)
→ OAP-1702B
→ LN-830U
→ 1906VA
→ 1781EW+
→ LN-830E
→ LN-830E+
→ 1790EF
→ 884 VoIP
→ R883+

4. Hinweise zu LCOS 10.94

Allgemeine Hinweise zum Update

Ab LCOS 10.90 wurde das CLI-Menü für VRRP von ‚/Setup/IP-Router/VRRP/' nach ‚/Setup/VRRP/' verschoben. Die Tabellenstruktur sowie der zugehörige OID-Pfad hat sich aufgrund der Unterstützung für VRRPv3 und IPv6 ebenfalls geändert.
Bitte beachten Sie, dass Add-Ins für die LMC sowie ggf. vorhande Scripte für VRRP für LCOS 10.90 und höher angepasst werden müssen. Existierende Scripte für VRRP sind nicht mit LCOS 10.90 und höher kompatibel.

Informationen zu Werkseinstellungen

Geräte, die mit LCOS 10.00 oder größer 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 über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

Unterstützung von eSIM

Die folgenden Produkte bzw. Hardware-Releases unterstützen die eSIM-Funktionalität ab LCOS 10.94:

- → LANCOM 1930EF-5G
- → LANCOM 1936VAG-5G
- → LANCOM OAP-5G
- → LANCOM 1800EF-4G (ab Hardware Release D)
- → LANCOM 1800EF-5G (ab Hardware Release D)
- → LANCOM 1800EFW-5G
- → LANCOM 1803VAW-5G
- → LANCOM 180xVA-4G (ab Hardware Release D)
- → LANCOM 180xVA-5G (ab Hardware Release D)

Die oben genannten Mobilfunkrouter (mit Quectel EM060K 4G-Modul und Quectel RM520N-GL 5G-Modul) müssen vor der Verwendung von eSIM auf die aktuelle WWAN-Firmware aktualisiert werden. Die aktuelle WWAN-Firmware finden Sie im Download-Bereich der jeweiligen Produkte.
Für den Einsatz von eSIM sind mindestens die folgenden Firmware-Versionen erforderlich:

- → Für 4G-Mobilfunkrouter mit Quectel EM060K:
  EM060KEAAAR01A05M2G_A0.300.A0.300-RU1
- → Für 5G-Mobilfunkrouter mit Quectel RM520N-GL:
  RM520NGLAAR03A03M4G_A0.301.A0.301-RU1

Schalter IPv4-WAN-Zugriff für interne DNS-Dienste

Ab LCOS 10.94 ist der Zugriff auf den DNS-Forwarder und DNS-Server für den IPv4-WAN-Zugriff global schaltbar. Die Konfiguration steht nach dem Update auf LCOS 10.94 auf „VPN“, d.h. dass der DNS-Dienst nur über LAN und VPN erreichbar ist. Als VPN gelten die Protokolle IKE/IKEv2/IPSec sowie WireGuard.

Dies führt dazu, dass der Zugriff auf die DNS-Dienste, in der der Router die Funktion des PPTP-, L2TP- sowie PPPoE-Servers hat, nicht mehr erlaubt ist. In diesem Fall ist eine manuelle Anpassung der Konfiguration nach dem Update erforderlich. Dies gilt nicht für den Fall, dass ein externer DNS-Server durch die Clients verwendet wird, sondern nur dort, wo der Router selbst DNS-Funktionen anbietet.

Neue Konfiguration für den DHCP-Client

Ab LCOS 10.94 entfallen die WAN- bzw. Kommunikations-Layer „DHCP“ und „B-DHCP“ (Broadcast-DHCP) in der Kommunikations-Layer-Tabelle. Die Konfiguration des DHCPv4-Clients erfolgt nun in der Tabelle DHCP-Client-Interfaces in LANconfig unter IPv4→DHCPv4→DHCP-Client. Dort muss nun für jedes WAN- und LAN-Interface ein Eintrag angelegt werden, auf denen der DHCP-Client aktiviert sein soll.

Ebenso wurde die Konfigurationsmöglichkeit des DHCP-Clients auf dem LAN aus dem DHCP-Server in die neue Tabelle verschoben. Der DHCP-Client wird nun somit an einer zentralen Stelle konfiguriert.

Bei einem Update auf LCOS 10.94 wird die Konfiguration automatisch auf das neue Format konvertiert.

Bitte beachten Sie, dass ein Downgrade auf ein Gerät mit LCOS kleiner als 10.94 dazu führen kann, dass ein Gerät mit einer DHCP-Client-WAN-Verbindung (z.B. WWAN-Verbindungen) keine Verbindung mehr herstellen kann, da keine Konvertierung der Konfiguration auf die alte DHCP-Konfiguration möglich ist. In diesem Fall muss eine Sicherung der Konfiguration eingespielt werden. Bitte beachten Sie hierzu auch die allgemeinen Hinweise zum Downgrade.

5. Feature-Übersicht LCOS 10.94

5.1 Feature-Highlights

eSIM: Die clevere Mobilfunklösung direkt im LANCOM Router

Mit der integrierten eSIM-Technologie verbinden sich LANCOM SD-WAN Gateways ganz unkompliziert mit dem Mobilfunknetz. Statt physischer SIM-Karten, die verwaltet und manuell ausgetauscht werden müssen, lassen sich Mobilfunkverträge und -profile einrichten und managen. Die fest im Gerät verbaute eSIM (Consumer-Variante) wird per Software mit dem Profil des Mobilfunkanbieters programmiert. So können Verträge oder Tarife schnell digital aufgespielt, gewechselt, aktualisiert und verwaltet werden – ganz ohne aufwändigen Kartenwechsel oder kostenintensive Vor-Ort-Einsätze. Neue Geräte sind sofort einsatzbereit; Rollouts an verschiedenen Standorten oder für viele Geräte lassen sich in kürzester Zeit durchführen. Gleichzeitig steigt die Sicherheit, da keine Karten verloren gehen oder missbräuchlich genutzt werden können. Ob für mobile Arbeitsplätze, Filialnetze oder als Backup-Lösung – eSIM ermöglicht die einfache Verwaltung der Mobilfunk-Konnektivität und bietet dabei ein Maximum an Flexibilität und Zeitersparnis.

WireGuard

Gerade in kleinen und überschaubaren Vernetzungsszenarien – etwa im Homeoffice oder in Unternehmen mit nur wenigen VPN-Anbindungen – bietet die Unterstützung von WireGuard eine schnell eingerichtete und zugleich flexible Lösung für eine sichere VPN-Verbindung. Dank seiner klaren Struktur und intuitiven Handhabung bietet das moderne Protokoll eine sichere und gleichzeitig unkomplizierte Lösung für einfache Vernetzungsszenarien. Moderne Kryptografie-Algorithmen sorgen dabei für eine zuverlässige Absicherung. WireGuard ermöglicht einen breiten Einsatz auf allen gängigen Betriebssystemen – ideal für heterogene IT-Umgebungen.

Zwei-Faktor-Authentifizierung (2FA)

Mit der Zwei-Faktor-Authentifizierung (2FA) wird das lokale Gerätemanagement unter LCOS nochmals deutlich sicherer. Neben der gewohnten Passworteingabe kann künftig ein zusätzlicher Sicherheitscode angefordert werden, der bequem über eine gängige Authenticator-App generiert wird. So bleibt der Zugriff selbst dann zuverlässig geschützt, wenn Ihr Passwort in falsche Hände geraten sollte. Die Einrichtung erfolgt unkompliziert mit Standard-Apps und bietet zusätzlich wirksamen Schutz vor Brute-Force-Attacken. Auf diese Weise erhöhen Sie Ihre Sicherheitsstandards, indem unerwünschte Gerätezugriffe abgewehrt werden.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 6 „Historie LCOS“.

6. Historie LCOS 10.94

LCOS-Änderungen 10.94.0274 RU3

Korrekturen / Anpassungen

Allgemein

→ Wenn eine SSH-Session oder ein CLI-Tunnel zu einem Router (Jumphost) gestartet und von diesem eine SSH-Session zu einem weiteren Router initiiert wurde, konnte es beim Übertragen größerer Datenmengen dazu kommen, dass die empfangenen Pakete des SSH-Clients auf dem Jumphost nicht ausgelesen wurden. Dies führte dazu, dass die SSH-Session einfror und keine Daten mehr übertragen werden konnten.
Verblieb der Jumphost in diesem Zustand ohne die Session manuell abzubauen, führte dies zu einem unvermittelten Neustart des Routers.

→ OpenSSL wurde auf die Version 3.5.6 aktualisiert. *

→ Nach dem Erstellen eines Zertifikats per Smart Certificate verbleibt der Assistent auf der Seite ‚Zertifikat erstellen', sodass direkt ein weiteres Zertifikat erstellt werden kann. Bei der Erstellung eines weiteren Zertifikates wurde die Session beendet und die Meldung „Access Forbidden" ausgegeben.

→ Bei Verwendung der Geräte-Login-Authentifizierung per RADIUS oder TACACS+ wurden dem Benutzer bei der Anmeldung per WEBconfig keine Rechte zugewiesen. Dies führte dazu, dass die Anmeldung mit der Fehlermeldung „Access Forbidden" abgelehnt wurde.

→ Der Netzwerk-Chip der SFP+-Ports des LANCOM ISG-8000 interpretierte UDP-Pakete ohne Prüfsumme so, als wäre die Prüfsumme fehlerhaft (packet checksum invalid). Wenn über eine VPN-Verbindung mit UDP (IPSec oder WireGuard) TCP-Anfragen auf interne Dienste des ISG-8000 (z.B. per SSH) gestellt wurden, übernahm der TCP-Stack des ISG-8000 die fehlerhafte Prüfsumme (Bad TCP checksum). Dies führte dazu, dass über eine VPN-Verbindung mit UDP keine TCP-Kommunikation mit dem ISG-8000 möglich war, wenn die Daten über die SFP+-Ports übertragen wurden.

→ Wenn bei einem LANCOM 1640E / 1650E bzw. einem Router der 179x- oder 192x-Serie zwei Ethernet-Ports unterschiedlichen LAN-Interfaces zugeordnet und diese in einer Bridge-Gruppe zusammengefasst wurden, konnte der Router ARP-Reply-Pakete nicht korrekt weiterleiten und verwarf diese. Dies führte dazu, dass die Kommunikation innerhalb des Netzwerks eingeschränkt war.

* LANCOM Systems 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.

→ WEBconfig erlaubte im Menü ‚Konfiguration / IP-Router / VRRP' nur maximal 15 Zeichen in den Feldern ‚Virt.-Link-Lokale-IPv6-Adr.' und ‚Virtuelle-Globale-IPv6-Adr.'.

→ Wenn bei einem eSIM-fähigen Mobilfunkrouter mehr eSIM-Profile in WEBconfig angelegt wurden, als es das Maximum erlaubte, wurde die Profil-Erstellung zwar abgelehnt, es erschien jedoch eine Fehlermeldung, die den Grund der Ablehnung nicht korrekt wiedergab.

→ Kam es beim Erstellen eines neuen eSIM-Profils in WEBconfig zu einem Fehler, führte das erneute Laden der eSIM-Verwaltungsseite dazu, dass die Seite ohne Inhalt angezeigt wurde.

→ Wenn der Router OpenSSL aktiv verwendete (z.B. im Rahmen der ‚Layer 7-Anwendungserkennung') konnte es vorkommen, dass ein Funktionszeiger keinen Wert hatte (Null). Dies führte zu einem unvermittelten Neustart des Gerätes.

→ Bei Verwendung eines Mobilfunk-Routers im Bridge-Modus wurden für die Übertragung von Informationen an das Mobilfunk-Modem Reservierungen im LAN-Pufferspeicher vorgenommen, der reservierte Puffer allerdings nicht wieder freigegeben. Nach einiger Laufzeit führte dies dazu, dass der LAN-Pufferspeicher voll und somit keine Datenübertragung im LAN mehr möglich war.

→ Nach einem Update auf LCOS 10.94 funktionierte der SMS-Versand per LANmonitor nicht mehr. Im LANmonitor wurde die Fehlermeldung „Rückgängig machen fehlgeschlagen." ausgegeben.

VoIP

→ Wenn der Voice Call Manager versucht, die SIP-Registrierung über eine IP-Adresse bei einem externen oder einem per VPN erreichbaren SIP-Server vorzunehmen, bevor die Internet-Verbindung bzw. die VPN-Verbindung aufgebaut ist, schlägt die Registrierung erwartungsgemäß fehl. Nach dem Aufbau der Internet- bzw. VPN-Verbindung wurde allerdings kein erneuter Registrierungs-Versuch durchgeführt. Dies führte dazu, dass die SIP-Telefonie nicht funktionierte.

→ Nach einem eingehenden Telefonat mit anschließender erfolgreicher Weiterleitung an einen anderen Teilnehmer konnte es vorkommen, dass der Voice Call Manager fälschlicherweise annahm, dass das Weiterleitungs-Ziel nicht antwortete. Dies führte dazu, dass der Voice Call Manager das Telefonat nach ca. 30 Sekunden mit einem CANCEL beendete.

→ Wenn bei der automatischen Signalisierungs-Verschlüsselung (Einstellung ‚Automatisch') UDP ohne Verschlüsselung ausgewählt wurde, versendete der Voice Call Manager bei einem ausgehenden Telefonat fälschlicherweise ein INVITE mit Krypto-Attributen.

WLAN

→ Empfing ein Access Point mit aktiver ‚ARP-Behandlung' ein Paket ohne IP-Header, konnte es vorkommen, dass im ARP-Handling die IP-Adresse aus dem IP-Header des vorigen Paketes verwendet wurde. Dies führte dazu, dass in der ARP-Tabelle für einen WLAN-Client die IP-Adresse eines anderen WLAN-Clients hinterlegt wurde (diese IP-Adresse wurde dem WLAN-Client aber nicht per DHCP zugewiesen). Durch den IP-Adresskonflikt war die Kommunikation der betroffenen WLAN-Clients nur noch eingeschränkt möglich.

LCOS-Änderungen 10.94.0217 RU2

Neue Features

→ Im SCEP-Client kann die Prüfung der aufgerufenen URL gegen die Server-Identität im TLS konfiguriert werden.

→ Für den WWAN-Bridge-Modus gibt es nun eine Status-Tabelle.

→ Über den neuen Parameter ‚Query-Timeout-ms' im DNS-Forwarder kann ein Timeout in Millisekunden eingestellt werden, bei dessen Ablauf der Forwarder den nächsten DNS-Server auswählt.

Korrekturen / Anpassungen

Allgemein

→ Beim Wechsel in den Cold-Standby wird die Stromversorgung für die SIM-Karte abgeschaltet, weshalb die PIN nach dem Wechsel in den aktiven Zustand erneut eingegeben werden muss. Dabei merkte der Router sich, dass die SIM bereits entsperrt wurde, setzte den Status beim Wechsel in den Cold-Standby aber nicht zurück. Dies führte dazu, dass die Mobilfunk-Verbindung nach dem Wechsel vom Cold-Standby in den aktiven Zustand nicht mehr aufgebaut werden konnte.

→ Beim Neustart des Mobilfunk-Modems auf Routern mit Sierra EM/MC7421 Mobilfunkmodem wurde fälschlicherweise ein Entfernen der SIM-Karte signalisiert. Wenn eine SIM-Karte während des Neustarts des Mobilfunkmodems entfernt oder eingesetzt wurde, konnte dies zu wiederholten unvermittelten Neustarts des Routers führen.
Die folgenden Mobilfunk-Router waren von diesem Verhalten betroffen:
- 1790-4G+
- 1790VA-4G+
- 1793VA-4G+
- 1800VAW-4G
- 1800VA-4G
- 1803VA-4G
- 1926VA-4G

→ Wenn eine Telekom Internet-Verbindung mit individuellem PPP-Benutzer oder mit dem alten Standard-Benutzer ‚internet-default@t-online.de' zuerst über den Setup-Assistenten ‚Gegenstelle oder Zugang löschen' entfernt und anschließend mit LANconfig 10.94 RU1 eine Internet-Verbindung mit dem neuen Standard-Benutzer ‚5200...' erstellt wurde, brach die Verbindung zum ACS-Server der Telekom mit dem Fehlercode „9005" ab.

→ Bei einem Wechsel des SIP-Servers verwendete der Voice Call Manager weiterhin den mit dem ersten SIP-Server ausgehandelten ‚REGISTER Expires'-

Wert. Dies konnte dazu führen, dass bei jedem Re-Register eine zusätzliche Aushandlung für den ‚REGISTER Expires'-Wert erfolgen musste.

→ Bei der Konfiguration eines RADIUS-Accounting-Servers in einem Public Spot Szenario wurde in der ‚Accounting-On'-Nachricht, welche für die Aktivierung des Accountings zuständig ist, ein defekter Wert für ‚Acct-Status-Type' gesendet.

→ Zur Behebung von CVE-2026-27171 wurde die zLib-Bibliothek auf die Version 1.3.2 aktualisiert. *

→ Wenn über die WebConfig-Oberfläche ein SNMP-Benutzer angelegt wurde und im Anschluss versucht wurde, über diesen Benutzer den LANCOM Router via LANmonitor oder eine andere SNMP-verwendende Software auszulesen, funktionierte dies nicht. Der Zugriff funktionierte erst, nachdem der per WebConfig angelegte Benutzer gelöscht und dieser im Anschluss über die Kommandoteile oder per LANConfig erneut angelegt wurde.

VPN

→ Nach dem Schreiben der Geräte-Konfiguration auf den Router (per LANconfig, WEBconfig oder per LMC) brachen alle VPN-Verbindungen ab.

→ Wenn eine LANCOM R&S®Unified Firewall bei einer bestehenden IKEv2-Verbindung zu einem LANCOM Router das Rekeying initiierte, konnte es dazu kommen, dass die IKEv2-Verbindung getrennt wurde.

WLAN

→ Nach einem Firmware-Update eines WLAN-Controllers (oder Routers mit WLC-Basic Option) auf LCOS 10.94 konnte es vorkommen, dass der Konfig-Konverter in den Verschlüsselungs-Profilen für den Parameter ‚Beacon-Sicherung' einen fehlerhaften Wert hinterlegte. Dies führte dazu, dass die verwalteten Access Points im LANmonitor einen Konfigurationsfehler meldeten und WLAN-Netzwerke mit WLC-Tunnel nicht mehr funktionsfähig waren.
Weiterhin konnte die Konfiguration des WLAN-Controllers per LANconfig nicht mehr geschrieben werden. LANconfig gab dann einen fehlerhaften Wert für den Parameter ‚1.2.37.1.1.1.60' an.

→ Bei Verwendung von 802.11r setzte jeder WLAN-Controller seine eigene MAC-Adresse als R0KH-ID ein. Dies führte in einem WLC-Cluster-Szenario dazu, dass 802.11r nicht korrekt funktionierte.

* LANCOM Systems 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.

→ Für die R0KH-ID wird jetzt immer der String „CAPWAP“ verwendet.

→ In einem WLAN-Controller-Szenario wurden Änderungen an den Interfaces (z.B. durch Wechsel von WLC-Tunnel auf ‚LAN am AP‘ oder Löschen bzw. Hinzufügen von SSIDs) nicht von den Access Points übernommen. Dies führte dazu, dass die Kommunikation in einigen oder sogar allen SSIDs nicht möglich war.

LCOS-Änderungen 10.94.0162 RU1

Neue Features

→ Eigene VRRP Advertisements werden nun im Fehlerfall bei einer Netzwerkschleife ignoriert und es wird eine entsprechende Syslog-Meldung erzeugt.

Korrekturen / Anpassungen

Allgemein

→ Wenn es in einem BGP-Szenario zwei gleiche Routen in der RIB-Tabelle gab (eine statische Route auf ein lokales LAN-Interface und eine von einem anderen BGP-Router empfangene), wurde die empfangene Route nicht entfernt, wenn das lokale LAN-Interface inaktiv war.

→ Zur Behebung von CVE-2025-1118 wurde die OpenSSL-Bibliothek auf die Version 3.5.5 aktualisiert. *

→ In LCOS 10.94 ist der Layer ‚DHCPOE' für Internet-Verbindungen entfallen. Stattdessen gibt es jetzt die Tabelle ‚DHCP-Client-Interfaces' im Menü ‚IPv4 → DHCPv4'. In dieser sind alle Internet-Verbindungen enthalten, die DHCP verwenden, u.a. die Standard-Verbindung ‚INTERNET-DEFAULT'. Da Einträge in den ‚DHCP-Client-Interfaces' Vorrang gegenüber einer statischen Konfiguration (IPoE) haben, führte dies bei Verwendung der Internet-Gegenstelle ‚INTERNET-DEFAULT' mit statischer Konfiguration nach einem Firmware-Update auf LCOS 10.94 Rel dazu, dass diese Verbindung nicht mehr funktionsfähig war.
Der Konfigurations-Konverter löscht jetzt zuerst die Tabelle ‚DHCP-Client-Interfaces' und fügt erst danach die Internet-Verbindungen, welche DHCP verwenden, hinzu.

→ Bei einem Firmware-Update von LCOS 10.80 auf LCOS 10.94 konnte es vorkommen, dass die Konverter für die konfigurierten Mobilfunk-Verbindungen nicht in der richtigen Reihenfolge ausgeführt wurden. Dies führte dazu, dass das ‚DHCP-Client-Interface' für die Mobilfunk-Verbindung nicht angelegt wurde und somit die Mobilfunk-Verbindung nicht funktionsfähig war.

VPN

→ WireGuard-Pakete wurden im ‚WG-Packet'-Trace mehrfach angezeigt.

→ Die IKEv2-Verschlüsselungs-Algorithmen AES-CBC und AES-GCM bzw. ChaChaPoly wurden in einem gemeinsamen ESP-Proposal gesendet, statt standardkonform in getrennten Proposals.

* LANCOM Systems 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-Änderungen 10.94.0127 Rel

Neue Features

WLC

→ Das Access Point-Lizenzlimit des LANCOM 2100EF wurde auf 60 angehoben.
→ Die Ziel-Sendeleistung lässt sich nun pro Access Point separat konfigurieren.
→ Die WLAN-Verschlüsselungseinstellungen werden nun in Verschlüsselungs-Profilen vorgenommen. Bestehende Konfigurationen werden beim Upgrade konvertiert.
→ Entfall von AutoWDS

Korrekturen / Anpassungen

Allgemein

→ Bei gleichzeitiger Verwendung mehrerer Dienst-Objekte und einem DNS-Ziel in einer Firewall-Regel wurde das DNS-Ziel nicht berücksichtigt.
→ Im Syslog eines LANCOM 2100EF wurde bei Meldungen zur Temperatur fälschlicherweise ein Hinweis zu einem WLAN-Modul ausgegeben „Temperature is back to normal, wireless is turned on again.“.
→ Der Status des Info-Feldes ‚Remote-Tables-Last-Change‘ im Konsolen-Pfad ‚Status/LLDP‘ wurde nicht korrekt verarbeitet, wenn dieses leer war (Null). Bei Auslesen des Konsolen-Pfads ‚Status/LLDP‘ führte dies dazu, dass die CPU-Last dauerhaft auf 100 % anstieg.
→ Wurde nach einem IDS- / DoS-Ereignis eine IDS- / DoS-Meldung durch die Firewall versandt, konnte dies zu einem unvermittelten Neustart des Routers führen.
→ Mit dem Parameter ‚-E‘ kann der iPerf-Client auf der Konsole auf eine bestimmte Internet-Gegenstelle eingeschränkt werden. Wurde dieser Parameter auf einem Router mit konfiguriertem Loadbalancer angewandt, verwendete der iPerf-Client alle Gegenstellen im Loadbalancer, statt diesen auf eine Verbindung einzuschränken. Dies führte zu fehlerhaften Messungen.
→ Durch einen Wechsel im Dateinamen-Format konnten Updates für den BPJM-Filter zwar heruntergeladen, aber nicht entpackt werden. Im Konsolen-Pfad ‚Status/Firewall/BPJM/Last-update-result‘ wurde dann die Meldung „Info-Request-failed“ ausgegeben. Dies führte dazu, dass der BPJM-Filter nicht funktionsfähig war.

→ Nach einem Scan des Mobilfunk-Netzwerks mit dem Konsolen-Befehl „do Scan-Networks -e -f“ konnte es auf dem LANCOM 1800EF-4G, 1800VA-4G und 1803VA-4G vorkommen, dass das Mobilfunkmodem für ca. 28 Minuten im Status ‚Registration Denied‘ verblieb, obwohl die Anmeldung im Mobilfunk-Netzwerk erfolgreich war.

VPN

→ WireGuard-Daten (sowohl IPv4 als auch IPv6) wurden nicht im Volumen-Budget berücksichtigt.

→ Dauerte die DNS-Auflösung der WireGuard-Gegenstelle zu lange, scheiterte der erste Verbindungsaufbau.

→ Wenn ein Router als WireGuard-Responder fungierte und bereits Pakete über die WireGuard-Verbindung in das Netzwerk des Responders gesendet wurden, bevor die WireGuard-Verbindung in den Status ‚Connected‘ wechselte, empfing der Responder die Pakete zwar und leitete diese auch weiter. Allerdings wurden die Antwort-Pakete blockiert und nicht weitergeleitet. Dadurch war die Kommunikation erst möglich, wenn die WireGuard-Verbindung in den Status ‚Connected‘ wechselte, was einige Sekunden dauern konnte.

LCOS-Änderungen 10.94.0093 RC2

Neue Features

→ Neuer Schalter ‚Always on' für WireGuard-Gegenstellen

→ Das BGP-Passwort kann nun bis zu 254 Zeichen lang sein.

→ Unterstützung für RADIUS-Bandbreiten-Limits im PPPoE-Server durch LANCOM-Vendor-Attribute LCS-TxRateLimit (2356-8) und LCS-RxRateLimit (2356-9).

Korrekturen / Anpassungen

Allgemein

→ Wenn bei einem LANCOM 1640E / 1650E bzw. einem Router der 179x- oder 192x-Serie zwei Ethernet-Ports unterschiedlichen LAN-Interfaces zugeordnet und diese in einer Bridge-Gruppe zusammengefasst wurden, konnte der Router ARP-Reply-Pakete nicht korrekt weiterleiten und verwarf diese. Dies führte dazu, dass die Kommunikation innerhalb des Netzwerks eingeschränkt war.

VPN

→ Eine WireGuard-Verbindung wurde in der Router-Firewall durch eine ‚Allow-VPN'-Regel (IPv4 - Bedingung ‚für VPN-Route', IPv6 - Aktionsobjekt ‚ACCEPT-VPN') nicht als VPN-Verbindung erkannt. Dies führte dazu, dass bei einer WireGuard-Verbindung zwischen zwei Routern der IPv4- und IPv6-Datenverkehr durch die ‚DENY-ALL'-Regel des Ziel-Routers blockiert wurde.

→ Bei einer Datenübertragung von IPv4-Paketen über eine IPv6-Verbindung per WireGuard zwischen zwei Routern konnte es vorkommen, dass die Checksumme des IPv4-Headers fehlerhaft berechnet wurde. Dadurch wurde das Paket verworfen und der Vorgang im WG-Packet-Trace mit der Fehlermeldung „Discarded, decapsulate wrong v4 header checksum" quittiert.

WLAN

→ Nach einer Aktualisierung auf LCOS 10.94 RC1 war ein fehlerhafter Standard-Parameter im Pfad ‚Setup / WLAN-Management' vorhanden. In der Folge konnte die Konfiguration des Gerätes mit LANconfig nicht mehr bearbeitet werden.

LCOS-Änderungen 10.94.0064 RC1

Neue Features

Allgemein

→ Unterstützung für Wireguard
→ Unterstützung für eSIM
→ Zwei-Faktor-Authentifizierung für die lokale Anmeldung am Router über WEBConfig, SSH, Telnet, TFTP sowie Outband
→ Unterstützung des Hybrid Post-Quantum-Algorithmus mlkem768×25519-sha256 im SSH
→ Unterstützung von Hybrid Post-Quantum ECDHE-MLKEM Key Agreement für TLSv1.3 (X25519MLKEM768)
→ Der DHCP-Client wird nun mit einem notwendigen Eintrag pro Interface in einer eigenen DHCP-Client-Tabelle konfiguriert.
→ Unterstützung der Parameter Framed-IP-Address, Framed-IPv6-Prefix, Delegated-IPv6-Prefix und Framed-IPv6-Address in der RADIUS-Server-Benutzertabelle
→ Die Syslog-Meldung bei Intrusion Detection wurde um Informationen des betroffenen Netzes ergänzt.
→ Der LMC-Status kann im WEBconfig-Dashbaord angezeigt werden.
→ E-Mail-Benachrichtigung bei fehlgeschlagenem ACME-Abruf und vor Ablauf des Zertifikates
→ Unterstützung von Q-in-Q-VLANs im PPPoE-Server
→ Wird vom Provider eine ‚LINE-ID' (Anschlussidentifikation) im PPP übermittelt, so wird diese im Status ausgegeben.
→ APN-Zugangsdaten (Benutzername, Passwort, Authentifizierungsmethode) können nun direkt im WWAN-Profil hinterlegt werden, statt über einen zusätzlichen Eintrag in der PPP-Tabelle. Die Konfigurationsmöglichkeit in der PPP-Tabelle bleibt weiterhin bestehen.
→ Der LANCOM 2100EF unterstützt in der WLC-Funktion nun einen Maximalausbau von 60 Access Points durch entsprechende zusätzliche Lizenzen.
→ Unterstützung der neuen Variable %w für die Aktionstabelle, mit der das IPv6-LAN-Präfix mit einem statischen Interface-Identifier kombiniert werden kann
→ Unterstützung für eine Historie der letzten Befehle in der CLI
→ Unterstützung für frei konfigurierbare Alias-Kommandos in der CLI
→ Verwendung des Firmsafe-Testmodus bei Firmware-Updates über die LMC
→ Unterstützung von RADIUS Change of Authorization (CoA) für den 802.1X Ethernet-Port Authenticator

→ Konfigurationsmöglichkeit der MTU in der Load-Balancer-Tabelle
→ Unterstützung von DSL Forum Vendor-Specific RADIUS-Attributen nach RFC-4679 im PPPoE-Server sowie Übermittlung an einen RADIUS-Server
→ Show-Kommando für PPPoE-User-Detail im PPPoE-Server
→ Die Gerätesuche in der WEBconfig gibt die Ergebnisse nun sortiert nach IP-Adresse aus.
→ Die interne WWAN-Carrier-Datenbank für die Auswahl der automatischen APNs wurde aktualisiert.
→ Schalter für den IPv4-WAN-Zugriff für interne DNS-Dienste
→ Unterstützung des WWAN-Bridge-Modus

WLC

→ Unterstützung für den Parameter ‚Beacon Protection' im Netzwerkprofil des WLCs
→ Unterstützung von neuen Wi-Fi 7-Access Points im zentralen Firmware-Managements des WLCs
→ Unterstützung der MLO-Konfiguration für Wi-Fi 7 im WLC

VoIP

→ Manipulation der Quellrufnummer bei abgehenden Rufen an Company-Flex-Anschlüssen
→ Sicherstellung eines freien Sprachkanals bei definierten Notrufnummern

Entfall

→ Die WAN-Layer DHCP und B-DHCP (Broadcast DHCP) entfallen. Der DHCP-Client wird nun mit einem notwendigen Eintrag pro Interface in einer eigenen DHCP-Client-Tabelle konfiguriert.
→ Entfall der Konfiguration des DHCP-Client-Modus in der Tabelle des DHCP-Servers
→ Entfall von AutoWDS
→ Der Parameter ‚Exklusiv' bei WAN-RADIUS-Server Operating entfällt.
→ Der Schalter ‚Max-WAN-Queue-Length' entfällt.
→ Die Unterstützung für das LANCOM Battery Pack entfällt.
→ Entfall der Vererbung in der WLC-Profil-Konfiguration

Korrekturen / Anpassungen

Allgemein

→ Die Programmbibliothek ‚jsPDF' wurde auf die Version 3.0.2 aktualisiert, wodurch die im CVE-2025-57810 beschriebene Sicherheitslücke behoben wurde.

→ Der SFP-Trace (trace # SFP) konnte auf dem R903 nicht ausgeführt werden, obwohl der R903 über einen SFP-Port verfügt.

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-Version unbedingt Ihre Konfigurationsdateien!

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

Wenn Sie Geräte, die Sie über eine Router-Verbindung oder WLAN-Punkt-zu-Punkt-Verbindung erreichen können, aktualisieren möchten, bedenken Sie bitte, dass Sie zuerst das entfernte LANCOM Gerät und anschließend das lokale LANCOM Gerät aktualisieren. Eine Anleitung zur Firmware-Aktualisierung erhalten Sie im LCOS-Referenzhandbuch. **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.

Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umständen nicht mehr möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Um mehr Platz im Speicher zu schaffen, muss dann statt einer vollwertigen Firmware zunächst eine eingeschränkte, kleinere Firmware eingerichtet werden. Hierdurch steht für die andere Firmware im Gerät erheblich mehr Speicher zur Verfügung. Diese Einrichtung ist nur einmalig erforderlich und wird mit einer „Minimalfirmware“ durchgeführt. Nach dem Einspielen der Minimalfirmware steht die Firmsafe-Funktion des LANCOM nur noch in eingeschränktem Umfang zur Verfügung. Das Update auf eine neuere Firmware ist weiterhin problemlos möglich. Das LANCOM Gerät arbeitet nach einem fehlgeschlagenen Update jedoch mit einer Minimalfirmware, die Ihnen ausschließlich den lokalen Zugriff auf das Gerät erlaubt. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.