

Release Notes

LCOS 10.92 RU1

Inhaltsübersicht

02	1. Einleitung
02	2. Das Release-Tag in der Software-Bezeichnung
03	3. Gerätespezifische Kompatibilität zu LCOS 10.92
03	LANCOM Geräte ohne Unterstützung ab LCOS 10.92
03	4. Hinweise zu LCOS 10.92
03	Allgemeine Hinweise zum Update
04	Informationen zu Werkseinstellungen
05	5. Feature-Übersicht LCOS 10.92
05	5.1 Feature-Highlights
05	Netzwerksicherheit aus der Cloud mit der LANCOM Security Essentials Option
06	6. Historie LCOS 10.92
06	LCOS-Änderungen 10.92.0098 RU1
09	LCOS-Änderungen 10.92.0018 Rel
11	7. Allgemeine Hinweise
11	Haftungsausschluss
11	Sichern der aktuellen Konfiguration
11	Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes



1. Einleitung

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

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.92 RU1 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 LANCOS 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 LANCOS 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 LANCOS Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS 10.92

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 unterstützte LCOS-Version für Ihr Gerät finden Sie unter

www.lancom.de/produkte/firmware/software-lifecycle-management

LANCOM Geräte ohne Unterstützung ab LCOS 10.92

- LANCOM R800V
- LANCOM LN-630acn
- LANCOM 1781VA
- LANCOM 1906VA-4G
- LANCOM L-322agn (R2)
- LANCOM LN-862
- LANCOM LN-860
- LANCOM OAP-830
- LANCOM OAP-1700B
- LANCOM OAP-821
- LANCOM OAP-822
- LANCOM IAP-1781VAW(+)

4. Hinweise zu LCOS 10.92

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. vorhandene Skripte für VRRP für LCOS 10.90 und höher angepasst werden müssen. Existierende Skripte 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.



5. Feature-Übersicht LCOS 10.92

5.1 Feature-Highlights

Netzwerksicherheit aus der Cloud mit der LANCOM Security Essentials Option

Mit LCOS 10.92 erfüllen Sie alle Voraussetzungen, um Ihre Geräte mit der LANCOM Security Essentials Option aufzurüsten. Die LANCOM Security Essentials Option bietet eine effiziente und zuverlässige Lösung, um Netzwerke vor Bedrohungen wie Ransomware, Phishing, Malware oder Diebstahl von Zugangsdaten zu schützen. Durch den integrierten Content Filter werden unerwünschte und illegale Internetinhalte gezielt blockiert – so bleibt die Integrität des Unternehmens gewahrt und das Haftungsrisiko wird deutlich reduziert. Gleichzeitig schützt das BPjM-Modul der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) Minderjährige zuverlässig vor jugendgefährdenden Inhalten. Die zugrunde liegende Datenbank zur Überprüfung der Webseiteninhalte wird DSGVO-konform in einer vertrauenswürdigen Cloud des europäischen Security-Spezialisten Bitdefender gehostet. Für beste Skalierbarkeit ist die Nutzung der Option nicht auf eine bestimmte Nutzeranzahl begrenzt – ideal für wachsende Netzwerke.

Hinweis: Die LANCOM Security Essentials Option ist als Upgrade-Option für LANCOM SD-WAN Gateways, SD-WAN Central Site Gateways und WLAN-Controller verfügbar und das Nachfolgeprodukt des LANCOM Content Filter.

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

6. Historie LCOS 10.92

LCOS-Änderungen 10.92.0098 RU1

Neue Features

- Bei Verwendung der Dynamic Path Selection (DPS) wird der ICMP-Identifizierer jetzt nach jeweils 4096 Messungen geändert (bei dem Standard-Intervall von einer Sekunde entspricht das ca. 70 Minuten).
- Die Backoff-Zeit bei einem fehlgeschlagenen VPN-Tunnelaufbau ist auf der CLI konfigurierbar.
- SIP-ALG: PMTU-Reduktion und Fragmentierung werden nur dann durchgeführt, wenn die MaxTxRate kleiner 1 MBit/s ist. Sollte keine Bandbreite konfiguriert sein, wird nicht reduziert oder fragmentiert.
- Die Länderkennung für das LANCOM DECT N610 IP ist im Default ‚Europa‘ statt ‚undefined‘.
- Content Filter: Wird von einem Anwender ein Override ausgeführt, so gilt dies für die komplette Domäne und unabhängig vom verwendeten Protokoll. Damit funktioniert auch der direkte Aufruf nach einem HTTPS Redirect.

Korrekturen / Anpassungen

Allgemein

- Wenn ein Mobilfunk-Modul aufgrund eines Hardware-Resets neu startete, konnte es dazu kommen, dass der interne PIN-Status im LCOS nicht zurückgesetzt wurde. Dies führte dazu, dass das LCOS die SIM nicht mehr entsperren konnte und das Mobilfunk-Modul sich infolgedessen nicht mehr mit dem Mobilfunknetz verbinden konnte.
- Wenn es bei der Verwendung des internen HTTP-Servers (etwa zum Bereitstellen von Zertifikaten) über eine langsame Verbindung zu einer Zeitüberschreitung kam, führte dies zu einem unvermittelten Neustart des Routers.
- Wenn eine Konfiguration über die LMC mehrfach an ein Gerät ausgerollt wurde, welches sich im Offline-Zustand befand, hatte dies zur Folge, dass die TACACS+-Authentifizierung deaktiviert wurde.
- Bei Verwendung der LANCOM Security Essentials konnte es vorkommen, dass erlaubte bzw. als sicher eingestufte Anwendungen (z.B. Office 365) und Kategorien vom Content Filter dennoch geblockt wurden.
- Beim Auslesen des hexadezimalen Passworts des GPON-Moduls konvertierte der Router dieses in Kleinbuchstaben. Wurden im PON-Passwort (unter Schnittstellen / WAN / PON) Großbuchstaben verwendet, führte dies zu einer Dauer-Bootschleife des GPON-Moduls.

- Beim Löschen der ARP-Tabelle nach Ablauf der ‚ARP-Aging-Minutes‘ wird für jeden gelöschten Eintrag ein Aufruf an die Firewall gestellt, um bei betroffenen Sessions die ARP-Auflösung zu löschen. In größeren Szenarien mit vielen gleichzeitigen Sessions führte dies zu periodisch auftretenden kurzen Lastspitzen bei jedem zweiten Löschvorgang der ARP-Tabelle (bei dem Standard-Wert der ‚ARP-Aging-Minutes‘ von 15 Minuten also alle 30 Minuten). Dadurch konnte es zu kurzzeitigen Verbindungs-Problemen kommen. Das ARP-Aging hat jetzt ein Intervall von 30 Sekunden. Weiterhin wird die Anzahl der ARP-Einträge, die gleichzeitig gelöscht werden können, limitiert (kann über den Konsolen-Pfad ‚Setup / TCP-IP / ARP-Max-Remove‘ angepasst werden, Standard-Wert ist 25). Sollen mehr ARP-Einträge gelöscht werden und wird dadurch das ARP-Aging-Limit überschritten, erfolgt eine Reduktion des ARP-Aging auf 10 Sekunden.
- Bei einem in Hyper-V betriebenen vRouter wurden bei einer PPPoE-Verbindung die Checksummen für TCP und UDP fehlerhaft berechnet. Dies konnte je nach verwendeter Netzwerkkarte unter Anderem zu starken Paketverlusten führen.
- Wenn dem Router bei der PPP-Aushandlung eine IP-Adresse mit x.x.x.255 zugewiesen wurde und der Einwahl-Router des Internet-Providers diese IP-Adresse ebenso beanspruchte, verwarf der Router DNS-Antworten. Dies führte dazu, dass über den Router keine Internet-Verbindung aufgebaut werden konnte. Weiterhin konnte der Router keine Verbindung zur LMC aufbauen.
- Nach einem Firmware-Update eines LANCOM 1793VA-4G auf LCOS 10.90 konnte dieser mit Standard-Einstellungen des Mobilfunk-Profiles ‚WWAN-DEFAULT‘ keine Mobilfunk-Verbindung mehr aufbauen. Dadurch war kein Zero-Touch-Rollout mehr möglich.
- Wurde per WEBconfig in einer Firewall-Regel eine Aktion mit sehr vielen Zeichen hinterlegt, führte dies zu einem unvermittelten Neustart des Routers.
- Wurde bei einem in Proxmox betriebenen vRouter mit VirtIO-Netzwerkkarte für die Internet-Verbindung Datenverkehr mit vielen gleichzeitigen Sessions über die Internet-Verbindung geleitet (etwa ein Speed-Test), führte dies zu starken Paketverlusten oder sogar einem Abbruch der Internet-Verbindung.

WLAN

- Wenn im Setup-Assistent ‚WLC-Profil einrichten‘ eine 4-stellige VLAN-ID eingegeben wurde, konnte dies dazu führen, dass das Gerät nach dem Fertigstellen des Assistenten einen unvermittelten Neustart ausführte.

VoIP

- Der Voice Call Manager leitete ein Besetztzeichen nicht an ISDN- und Analog-Teilnehmer weiter.
- Nach einer Aktualisierung auf LCOS 10.9x konnte es vorkommen, dass sich ein SIP-Client über eine im Voice Call Manager eingerichtete SIP-PBX-Leitung nicht mehr an einer SIP-Telefonanlage (z.B. einer Cloud PBX) anmelden konnte.
- Auf der WEBconfig-Oberfläche eines LANCOM 1803VA war es nicht möglich, ISDN-Schnittstellen zu konfigurieren bzw. zu aktivieren.
- Empfang der Voice Call Manager bei einem ausgehenden Ruf ein ‚Provisional Update‘ von der SIP-TK-Anlage, sendete der Voice Call Manager anschließend ein PRACK mit „RAck: 2 100 UPDATE“ statt „RAck: 2 100 INVITE“ an den SIP-Provider. Dies führte dazu, dass der SIP-Provider die Verbindung mit der Meldung „481 Call/Transaction Does Not Exist“ abbaute.
- Der Voice Call Manager konnte mehrteilige SDP-Meldungen nicht verarbeiten und sendete dann die Meldung „406 SDP Not Acceptable“.
- Wurde von einem SIP-Benutzer ein Telefonat mit einem Video- und einem Audio-Stream zu einem ISDN- oder Analog-Benutzer aufgebaut, entfernte der Voice Call Manager den Video-Stream und deaktivierte den Audio-Stream (m=audio 0). Dies führte dazu, dass keine Sprach-Kommunikation möglich war. Der Voice Call Manager deaktiviert in einem solchen Szenario jetzt den Video-Stream und lässt den Audio-Stream aktiv.

LCOS-Änderungen 10.92.0018 Rel

Neue Features

- Unterstützung der LANCOM Security Essentials Option
- Wechsel des Content Filters auf Bitdefender
Bitte beachten Sie, dass sich durch den Wechsel die Kategorien teilweise verändert haben sowie neue Kategorien hinzugekommen sind. Es wird empfohlen, nach dem LCOS-Update die Konfiguration zu prüfen. Bitte beachten Sie dazu auch die [Hinweise zum Update](#).
- Unterstützung der Backup/Restore-Funktion des Geräts
- Unterstützung von Dynamic RADIUS-Caching
- Das Verhalten für den Inter-Tunnel-Verkehr kann bei L2TPv3 konfiguriert werden.

Korrekturen / Anpassungen

Allgemein

- Bei Verwendung einer unmaskierten Default-Route für eine IKEv2-Verbindung wurde fälschlicherweise angezeigt, dass der DNS-Server aus dem WAN erreichbar war.
- Der DSL-Linecode wurde bei den Geräten der 180xVA- und 1926/1936-Serien auf die Version 12.9.1.2.0.7 aktualisiert.
- Die Passwortänderung eines angemeldeten TACACS-Benutzers wurde in der WEBconfig mit der Fehlermeldung „Not Found“ quittiert. In der Folge schlug die Änderung des Passworts fehl.
- Beim wiederholten Auslesen des Konsolen-Pfads ‚Status/VDSL/Line-Type‘ (dies betraf auch den übergeordneten Pfad ‚Status/VDSL‘) mit dem Repeat-Befehl (z. B. „repeat 3 ls Status/VDSL/Line-Type“) wurden die Informationen nur einmalig ausgegeben.
- Wenn in einem VRRP-Szenario auf dem Standby-Router im DHCP-Netzwerk kein Gateway eingetragen wurde (0.0.0.0), sendete der Standby-Router ein DHCP-Offer ohne Gateway, statt die VRRP-IP-Adresse zu verwenden. Wenn ein Endgerät das DHCP-Offer zuerst vom Standby-Router empfing, statt vom Master-Router, akzeptierte dieses die zugewiesene IP-Adresse nicht und es war keine Kommunikation möglich.
- Wurde in einem OSPF-Szenario das VLAN eines Netzwerks - und damit auch das Routing-Tag des Netzwerks sowie der OSPF-Instanz - geändert, führte dies dazu, dass der OSPF-Neighbor anschließend im Status ‚down‘ verblieb und die Verbindung nicht wieder aufgebaut wurde.

VPN

→ Empfang ein Router mit mehreren aktiven Internet-Verbindungen und einer IKEv2-Verbindung mit einem bestimmten Routing-Tag ein IKE-Paket mit dem Message Type ‚Redirect‘, änderte der Router das Routing-Tag für das ausgehende IKE_SA_INIT auf 0, statt das bisherige Routing-Tag beizubehalten. Dies führte dazu, dass die VPN-Kommunikation anschließend über die falsche Internet-Verbindung übertragen wurde.

WLAN

→ Die IAPP-Tabelle kann maximal 2048 Einträge aufnehmen. Neue Access Points können daher bei Erreichen des Maximums nicht mehr hinzugefügt werden. Wenn ein Access Point nicht mehr in der IAPP-Tabelle hinzugefügt und daher in der Tabelle nicht gefunden werden konnte, führte dies zu einem unvermittelten Neustart des Access Points.

→ Wenn in der Tabelle ‚Setup/Public-Spot-Module/Free-Server‘ ein IP-Adress-Eintrag für einen frei erreichbaren Web-Server vorhanden war, kam es beim Aufruf einer HTML-Seite dieses Web-Servers aufgrund eines nicht vorhandenen HTML-Headers zu einer Fehlermeldung.

VoIP

→ Wenn die Kommunikation mit einem bestimmten Ziel nur über eine spezifische, dynamisch gelernte Route mit ‚Next Hop‘ (z. B. per BGP) möglich, zusätzlich aber noch eine statisch konfigurierte Default-Route ohne ‚Next Hop‘ für die gleiche Gegenstelle, aber mit einem anderen Routing-Tag konfiguriert war und der Router ein Paket für das Ziel-Netzwerk empfing, bevor die dynamische Route gelernt wurde, ersetzte der Router für die Session die statische nicht durch die dynamische Route (die statische Route wurde nicht invalidiert). Dies führte dazu, dass weiterhin die statische Route verwendet wurde und das Ziel-Netzwerk darüber nicht erreicht werden konnte.

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.