Release Notes

LCOS
10.92 RU6

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 10.92 RU6 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 10.92

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 unterstütze 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. 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.

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 10.92.0346 RU6

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 3.0.21 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.

→ 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.

→ 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.'.

* 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.

WLAN

→ In seltenen Fällen konnte es in einem WLC-Cluster vorkommen, dass die WLAN-Controller Pakete zur Verwaltung des Clusters nicht mehr austauschen konnten. Dies führte dazu, dass die Synchronisierung innerhalb des WLC-Clusters nicht mehr funktionierte.

→ In einem WLAN-Netzwerk mit 802.1X und mehreren RADIUS-Servern sowie aktiver RADIUS Pre-Authentifizierung (Standalone-Betrieb und LMC-managed) las der Access Point ein falsches Feld in den Verschlüsselungseinstellungen aus, weshalb immer der erste RADIUS-Server verwendet wurde. Wenn ein anderer RADIUS-Server erforderlich war, führte dies dazu, dass die Pre-Authentifizierung nicht funktionierte.
Bei aktiver Pre-Authentifizierung greift der Access Point jetzt auf das korrekte Feld in den Verschlüsselungseinstellungen zurück, sodass der korrekte RADIUS-Server verwendet wird.

VoIP

→ 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.

LCOS-Änderungen 10.92.0325 RU5

Korrekturen / Anpassungen

Allgemein

→ In LCOS 10.94 erfolgte ein Update auf OpenSSL 3.5. Dieses erfordert Certificate Signing Requests (CSR) in Version 1 und lehnt CSRs mit einer falschen Version ab. Access Points und WLAN-Router senden bis einschließlich LCOS 10.92 CSRs in Version 3 an den WLAN-Controller. Dies führte dazu, dass neu hinzugefügte Access Points und WLAN-Router mit LCOS bis einschließlich Version 10.92 kein Zertifikat von einem WLAN-Controller mit LCOS 10.94 beziehen und somit von diesem auch nicht verwaltet werden konnten (bereits verbundene Access Points und WLAN-Router sind nicht betroffen).

→ 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.
Dies betraf die folgenden LANCOM Router:

- 1800EF
- 1800EF-4G
- 1800EF-5G
- 1800EFW
- 2100EF
- vRouter
- ISG-5000
- ISG-8000
- WLC-2000

→ Ein per WEBconfig erstellter SNMP-Benutzer wurde unvollständig angelegt. Dies führte dazu, dass dieser nicht funktionsfähig war und im LANmonitor sowie andere SNMP-Monitoring-Software nicht verwendet werden konnte.

→ 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.

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

** LANCOM Systems hält alle in einer LCOS-Firmware verwendeten Programmbibliotheken auf dem

VPN

→ 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

→ 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.
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.

VoIP

→ 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.

aktuellen Sicherheitsstand und behebt Sicherheitslücken auch dann, wenn sie in der Firmware nicht ausnutzbar sind.

LCOS-Änderungen 10.92.0278 RU4

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.

→ Die Kommunikation von Clients innerhalb des gleichen Netzwerks erfolgt nativ über den Switch. Wenn Clients in verschiedenen Netzwerken, welche über verschiedene Ethernet-Ports angebunden waren, miteinander kommunizieren sollten, wurden die MAC-Adressen der Clients durch die LAN-Bridge dauerhaft dem CPU-Port zugewiesen. Sollte anschließend ein Client in einem der Netzwerke mit einem weiteren Client in dem gleichen Netzwerk kommunizieren, war dies nicht mehr möglich, weil die MAC-Adresse noch dem CPU-Port zugewiesen war. Die Pakete wurden daher durch die LAN-Bridge verworfen.

Dies betraf die folgenden Router-Modelle:

- 1800EFW-5G
- 1800EFW
- 1800EF-5G
- 1800EF

- 1800VA
- 1800VAW
- 1800VAW-4G
- 1800VAW-5G
- 1800VA-4G
- 1800VA-5G
- 1803VAW
- 1803VAW-5G
- 1803VA-4G
- 1803VA-5G
- R903
- 1930EF
- 1930EF-5G
- 1936VAG
- 1936VAG-4G
- 1936VAG-5G

→ Zur Behebung von CVE-2025-15467 wurde die OpenSSL-Bibliothek auf die Version 3.0.19 aktualisiert.

→ Bei aktiviertertem IGMP- und MLD-Snooping wurde im IPv6-Modus fälschlicherweise der Backup-Router zum VRRP-Master gewählt, da das Snooping die VRRP-Multicast-Adresse ff02::12 (VRRP-IPv6) blockierte.

→ War die maximale Größe der RADIUS-Benutzertabelle erreicht, lieferte der Public Spot-Assistent beim Erstellen eines neuen Public Spot-Benutzers statt einer aussagekräftigen Fehlermeldung eine ungültige Seite ohne HTTP-Header aus. Im Web-Browser wurde die Meldung „The Server provided an invalid message! Content Length: 0“ ausgegeben.

→ 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.

WLAN

→ In der Major-Version LCOS 10.90 wurde das Feature ‚Management-Rate' eingeführt, mit dem die Geschwindigkeit der Management-Beacon-Frames beeinflusst werden kann. In der Standard-Einstellung steht diese auf ‚Minimum', was bedeutet, dass die niedrigste Geschwindigkeit für den verwendeten WLAN-Standard verwendet wird (1 oder 6 MBit). Dabei wurde der für die ‚Management-Rate' verwendete Wert auch in das ‚Basic Rate Set' aufgenommen, also die Geschwindigkeit, die Clients unterstützen müssen, damit diese mit dem WLAN kommunizieren können. Dies führte dazu, dass WLAN-Analyse-Software die Geschwindigkeit der ‚Management-Rate' als ‚Minimale Basisrate' anzeigte, was stark von dem empfohlenen Wert abwich.

LCOS-Änderungen 10.92.0227 RU3

Korrekturen / Anpassungen

Allgemein

→ Der SFP-Trace „trace # SFP“ konnte auf dem LANCOM R903 nicht ausgeführt werden, obwohl das Gerät über einen SFP-Port verfügt.

→ Bei der Datenübertragung über eine Internet-Verbindung mit geringer Upstream-Datenrate kam es im Active Queue Management des Ethernet-Treibers zu einem Loop. Dies führte zu einer stark erhöhten CPU-Last während des Uploads.

→ Beim Download der Signatur-Updates für den BPJM-Filter schlug der Abgleich des lokalen Datei-Headers mit dem Central Directory Record der Zip-Datei mit dem Signatur-Update fehl. Dies führte dazu, dass das Signatur-Update nicht heruntergeladen werden konnte. Im LANmonitor wurde dazu die Fehlermeldung „Zip-Extraktion fehlgeschlagen“ angezeigt.

→ 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.

→ Zur Behebung einer Sicherheitslücke (CVE-2025-9230) wurde die OpenSSL-Bibliothek auf die Version 3.0.18 aktualisiert.

→ Die Programmbibliothek ‚jsPDF‘ wurde auf die Version 3.0.2 aktualisiert, um eine Sicherheitslücke (CVE-2025-57810) zu beheben.

→ In der LANCOM 1800EF-Serie waren die Standard-Einstellungen für die Bridge-Gruppen der Ports LAN-5 und LAN-6 nicht korrekt.

→ Erfolgte in einem Szenario mit aktiver Zugriffs-Verwaltung per RADIUS oder TACACS+ ein Upload der Konfiguration mit dem RADIUS- / TACACS+-Benutzer als *.lcf-Datei, war das Hauptgerätepasswort des Benutzers ‚root‘ im Backup-Fall leer und die Anmeldung nur ohne Passwort möglich.

→ Die Accounting-Tabellen wurden auf den folgenden LANCOM Router-Modellen nicht bootpersistent gespeichert und waren daher nach einem Neustart leer:

- 180x-Serie
- 1936VAG / 1936VAG-5G
- 2100EF
- ISG-5000 / ISG-8000
- vRouter

→ Erfolgt in einem VRRP-Szenario ein Wechsel des VRRP-Masters, sendet dieser ein Gratuitous ARP (GARP) mit der VRRP-MAC-Adresse in das Netzwerk. Bei gleichzeitiger Verwendung von VRRP und LACP mit benutzerdefinierter LACP-MAC-Adresse sowie aktiver LAN-Bridge sendete der neue VRRP-Master im GARP statt der VRRP-MAC-Adresse die LACP-MAC-Adresse. Dies führte dazu, dass die Kommunikation stark eingeschränkt war.

→ Ab LCOS 10.90 konnten auf LANCOM Access Points mit LCOS und WLAN-Routern der LANCOM 1700-Serie über DSLoL (DSL over LAN) keine Daten mehr übertragen werden.

→ Konnte der Public Spot Benutzer in der RADIUS-Benutzer-Tabelle beim Erstellen eines neuen Public Spot Vouchers nicht angelegt werden (etwa weil die Tabelle ‚Accounting-Total' voll war), führte dies zu einem unvermittelten Neustart.

→ Es konnte sporadisch zu unvermittelten Neustarts bei 5G-Routern kommen.

VPN

→ Nach einem gescheiterten Verbindungsversuch eines Geräts mit konfiguriertem IKEv2-EAP zu einem Router mit unkonfiguriertem IKEv2-EAP verblieb die aufgebaute Security Association (SA) in der Security Association Data Base (SADB) des Routers und wurde nicht mehr gelöscht.

→ Eine eingehende VPN-Verbindung in einem VRRP-Szenario ohne aktiven IKEv2-Loadbalancer konnte nicht aufgebaut werden, wenn die virtuelle VRRP-Adresse für den Aufbau verwendet wurde.

LCOS-Änderungen 10.92.0167 RU2

Korrekturen / Anpassungen

Allgemein

→ Bei konfiguriertem TACACS+ konnte es beim Öffnen der Portforwarding-Tabelle per WEBconfig zu einem unvermittelten Neustart des Routers kommen.

→ War das Netz des Mobilfunk-Providers in einem Fehlerzustand, erkannte der Router diesen und führte eine Reinitialisierung mit anschließendem Neustart des Mobilfunk-Modems durch, um aus dem Fehlerzustand wieder herauszukommen. Dies konnte einige Minuten dauern.
In einem solchen Fall wird jetzt ein Reattach des Mobilfunk-Modems durchgeführt und die Ausfallzeit somit minimiert.

VPN

→ Eine unter iOS 26 neu erstellte IKEv2-Verbindung konnte nicht aufgebaut werden, da ein neues iOS-Feature nicht mit LCOS kompatibel war.

WLAN

→ Bei Verwendung von Client-Steering (nicht empfohlen, stattdessen sollte Client-Management verwendet werden) konnte es in Umgebungen mit sehr vielen eingebuchten WLAN-Endgeräten zu einem unvermittelten Neustart des WLAN-Controllers kommen.

LCOS-Änderungen 10.92.0098 RU1

Neue Features

→ Bei Verwendung der Dynamic Path Selection (DPS) wird der ICMP-Identifier 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 eingestufe 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-Profils ‚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

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.

→ Empfing 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

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.