Informationen zur

LCOS Software Release 10.12 SU3

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

Internet: http://www.lancom.de

20.11.2017, CBuersch

Inhaltsübersicht

1. Einleitung

LCOS („LANCOM Operating System“) ist das Betriebssystem für alle LANCOM Router und Wireless LAN Access Points. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.12 SU3 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 3 dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite
https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/

2. Neue Features, Änderungen und Historie

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.

LCOS Änderungen von 10.12.0146 RU2 ► 10.12.0147 SU3

Korrekturen / Anpassungen

Security Update für LANCOM Router, Gateways, Access Points und WLAN Controller

- Das Update behebt eine sicherheitsrelevante Schwachstelle in den Management-Funktionen. Potentiell betroffen sind alle Geräte, die mit folgenden Firmware-Versionen laufen:
  - LCOS 10.12 REL, SU1, RU2
  - LCOS 10.10 RU2, 10.10.0165 PR, 10.10 RU4
  - LCOS 9.24 RU6, SU7, RU8

  Für diese Geräte wird das Update empfohlen. Alle anderen Versionen sind nicht betroffen.

LCOS Änderungen von 10.12.0084 SU1 ► 10.12.0146 RU2

Neue Features

- Der Treiber für das IEEE 802.11ac-Wave1-WLAN-Modul der folgenden Produkte wurde aktualisiert: LN-630acn dual Wireless, LN-830acn dual Wireless, L-1310acn dual Wireless, L-1302acn dual Wireless, IAP-821, IAP-822, OAP-821, OAP-822, OAP-830
- vRouter-Lizenzen des Typs "vRouter 500" können nun aktiviert werden.
- Zero-Touch-Provisionierung mit der LANCOM Management Cloud: LANCOM Router mit Ethernet-WAN-Port bauen im Auslieferungszustand eine DHCPoE-Verbindung über den WAN-Port auf und verbinden sich mit der LANCOM Management Cloud.

Korrekturen / Anpassungen

Allgemein

- Ein Schreiben der Konfiguration via LANconfig per TFTP oder serieller Schnittstelle war nicht möglich, wenn das LANCOM Gerät keine aktivierte Public Spot Option besaß.
- Ein Zurückschreiben der Konfiguration auf einem LANCOM Gerät ohne freigeschaltete Public Spot Option war über die serielle Schnittstelle nicht möglich.
- Beim LANCOM 1780EW-4G+ konnte eine konfigurierte WWAN-Verbindung (LTE oder UMTS) sporadisch nicht verwendet werden, weil das Mobilfunk-Modul keine IP-Adresse per DHCP mehr bezog.
- Auf Geräten vom Typ LANCOM 1780EW-4G+ konnte 2G (GPRS) als Fallback für Mobilfunkverbindungen konfiguriert werden, obwohl dieses Gerät es nicht unterstützt.
- Die LCOS-interne CA-Hierarchie, welche die Geräte-Zertifikate für HTTPS-Verbindungen auf das Gerät erstellt, war beim LANCOM 7100(+) VPN, 9100(+) VPN, WLC-4025+ und WLC-4100 fehlerhaft. Dies führte zu Geräte-Zertifikaten, welche vom Browser nicht akzeptiert wurden.
- Ein fehlgeschlagener SCEP-Request verhinderte das Ausführen weiterer SCEP-Requests, obwohl eine andere Zertifizierungsstelle angefragt werden sollte.
- Eine Verbindung zu einer DHCPoE-Gegenstelle konnte nicht aufgebaut werden, wenn das der Gegenstelle zugeordnete DSLoL-Interface einer Bridge-Gruppe zugeordnet war.
- Wenn das "iperf"-Kommando in der Komandozeile des LANCOM unvollständig oder abgekürzt eingegeben wurde (z.B. "iper" statt "iperf"), startete der iperf-Server mit einer Warnmeldung.
- Unter /Setup/DNS/DNS-Destinations konnten keine zwei Server als Ziel eingetragen werden, wenn einer oder beide mit dem '@'-Zeichen erweitert wurden. Mit dem '@'-Zeichen kann ein Routing-Tag mitgegeben werden.
- Im DHCP-Offer wurde einem BOOTP-Client der Server nicht übermittelt, welcher unter "Boot-Images" eingetragen war.
- Es konnten keine Objekte in der Firewall (LCOS-Menübaum: /Setup/IP-Router/Firewall/Objects; LANconfig: Firewall/QoS > IPv4-Regeln > Stations-Objekte) angelegt werden, welche das '@'-Zeichen enthielten, obwohl der erlaubte Zeichensatz das '@'-Zeichen einschließt.
- Es wurden Pakete, welche durch eine Firewall-Regel zurückgewiesen werden sollten, übertragen, wenn in der Firewall zwei QoS-Regeln mit jeweils aktivierter Verlinkung ("Weitere Regeln beachten, nachdem diese Regel zutrifft") aktiv waren und die Pakete auf eine dieser QoS-Regeln zutrafen.

VPN

- Es konnte sporadisch zu einem unvermittelten Neustart des Gerätes kommen, wenn der Zeitpunkt eines IPSec-Verbindungsabbaus mit dem Zustellen eines Datenpaketes, noch zugehörend zur abgebauten IPSec-Verbindung zusammenfiel.

- Es war nicht möglich, mehrere Dynamic VPN-Aushandlungen gleichzeitig auszuführen. Dies führte dazu, dass die zugehörigen VPN-Tunnel nicht aufgebaut werden konnten.

WLAN

- Eine in der Konfiguration hinterlegte Sendeleistungsreduktion auf dem IEEE 802.11ac-Modul wurde im Unterband 2 nicht berücksichtigt. Die Reduktion wurde auf den EIRP berechnet und nicht wie gewünscht auf die maximale Sendeleistung des Moduls.
- Die Funktion "Adaptive RF Optimization" wurde um die Nutzungs-Bewertung der Kanäle durch andere WLAN-Geräte erweitert.
- Der WPA-Rekeying Mechanismus funktionierte aufgrund einer fehlenden Rekeying-ID nicht ordnungsgemäß.

VoIP

- Eine SIP-Leitung konnte die Registrierung verlieren, wenn der DNS-Name des Registrars über einen DNS-Server aufgelöst wurde, der ein TTL=0 mitgeliefert hat.
- Das Setzen eines Anruf-Präfix auf einer SIP-Leitungs-Gegenstelle unter "Voice Call Manager > Leitungen > SIP-Leitungen > ..." führte zur Weitergabe der rufenden Nummer in einem ungültigen Format (z.B. 0+49), da die internationale Vorwahl von z.B. +49 nicht in 0049 geändert wurde.
- Wenn ein eingehender Voice-over-IP Anruf länger als 120 Sekunden signalisiert wurde, ohne angenommen zu werden, und dann vom Provider beendet wurde, verblieb der Ruf mit dem Status "Klingeln" in der Ruf-Liste.

LCOS Änderungen von 10.12.0082 Rel ► 10.12.0084 SU1

Korrekturen / Anpassungen

WLAN

- Es wurde eine Sicherheitslücke im WPA2-Verfahren (KRACK-Attacke) im Zusammenhang mit der Nutzung von 802.11r (Fast-Roaming) im AP-Betrieb (Basisstation) behoben:

  CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it

  Bitte informieren Sie sich zudem beim jeweiligen Hersteller über die Verfügbarkeit von Updates für Ihre WLAN-Clients. Auch diese Geräte müssen aktualisiert werden.

- Es wurde eine Sicherheitslücke im WPA2-Verfahren (KRACK-Attacke) im Zusammenhang mit der Nutzung des WLAN-Client-Modus / WLAN-Station-Mode mit 802.11ac-WLAN-Modulen, sowie bei Benutzung von Punkt-zu-Punkt-Strecken mit 802.11ac- und 802.11a/b/g/n-WLAN-Modulen behoben:

  CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
  CVE-2017-13080: reinstallation of the group key in the Group Key handshake

  Der mit 802.11a/b/g/n-WLAN-Modulen betriebene WLAN-Client-Modus / WLAN-Station-Mode ist nicht betroffen.

Hinweis:

Von den folgenden WPA2-Sicherheitslücken (KRACK-Attacke) ist das LCOS nicht betroffen:

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13078: reinstallation of the group key in the Four-way handshake
CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

LCOS Änderungen von 10.12.0059 RC2 ► 10.12.0082 Rel

Korrekturen / Anpassungen

Allgemein

- Nach einem Neustart des LANCOM Gerätes verblieben alle Ports im Status "disabled", obwohl Spanning Tree aktiviert war.
- Eine per DHCP-Option zugewiesene LMC-Domäne wurde vom LANCOM Gerät (DHCP-Client) ignoriert.
- Eine ADSL-Verbindung mit der Encapsulation VC-MUX und einem transparenten Layer-2 (anstelle von PPPoE) konnte nicht erfolgreich aufgebaut werden.

- Nach Ablauf der Lease-Time wurde auf einer Internet-Gegenstelle mit dem Layer DHCPoEoV keine neue IP-Adresse bezogen und die Verbindung wurde kurzzeitig unterbrochen.
- Wenn vom einen Server in der DMZ zu große Pakete (größer als die MTU der Ziel-Gegenstelle) an LANCOM Router gesendet wurden, in denen das DF-Bit (don't fragment) gesetzt war, so sendete der LANCOM Router keine ICMP-Fehlermeldung mit der Nachricht "fragmentation needed..." an den Sender der Pakete und verwarf diese.
- Wenn in der Netzwerk-Definition der LANCOM Management Cloud eine VLAN-ID eingetragen wurde, die gößer als 999 war, wurde diese Konfiguration nicht akzeptiert, obwohl VLAN-IDs bis 4094 in den Netzwerk-Definitionen erlaubt sind.
- Wenn ein NTP-Server im Netzwerk INTRANET konfiguriert war, so konnte die Konfiguration des Gerätes über LANconfig nach einer beliebigen Änderung nicht mehr zurückgeschrieben werden.
- Geroutete Multicasts (z.B. Videostream an DSL-1) wurden innerhalb einer Bridge-Gruppe (z.B. BRG-1) am IGMP-Snooping vorbei auf das Interface LAN-1 und, sobald ein Client im WLAN eingebucht war, auch auf WLAN-1 gebridged. Dies führte dazu, dass das WLAN mit Multicast-Paketen "überflutet" wurde und die WLAN-Kanallast derart anstieg. dass die WLAN-Verbindung nicht performant genug war.
- In einem VRRP Loadbalancing Szenario mit RIP wurden ICMP Redirects mit der Quell-IP-Adresse des ARF-Kontextes und nicht mit der VRRP-IP-Adresse versendet.
- In einem EoGRE-Tunnel, dem unter Schnittstellen -> LAN -> Port-Tabelle keiner Bridge-Gruppe zugewiesen wurde, wurden keine Daten übertragen.

WLAN

- Per AutoWDS konnte keine Punkt-zu-Punkt Verbindung zwischen LANCOM Access Points hergestellt werden. Die für AutoWDS eingetragenen Access Points wurden zwar in der entsprechenden SSID angezeigt (im LANmonitor), eine Verbindung kam jedoch nicht zustande.
- Clients, welche am LANCOM Public Spot initial angemeldet waren, konnten keine Verbindung zum WAN herstellen, da die DNS-Anfragen der initialen Domain nicht an ein vorgeschaltetes Gerät (welches den WAN-Zugang bereitstellte) weitergeleitet wurden.
- Beim Auslesen der Konfiguration eines LANCOM WLAN-Controller per LANconfig wurde das Wireless-IDS-Profil „Default" nicht mit ausgelesen. In der Folge konnte die Konfiguration nicht in den LANCOM WLAN-Controller zurückgeschrieben werden.

VoIP

- Wenn die Einrichtung eines All-IP Anschlusses im WEBconfig mit dem Setup-Assistent „Voice-over-IP / All-IP einrichten" vorgenommen wurde, blieb die eingerichtete ISDN-Schnittstelle nach Durchlauf des Assistenten im Schaltzustand „Aus".
- Wenn im LANCOM Voice Call Manager in den Einstellungen eines Benutzers (Voice Call Manager > Benutzer > Benutzer Einstellungen) die Funktion „Zweitanruf unterdrücken (Busy-on-Busy)" aktiviert war, wurden dem jeweiligen Benutzer keine Anrufe zugestellt.

VPN & Routing

- Eine IKEv2-Verbindung mit einen Digital-Signature-Profil „RSASSA-PSS mit SHA-384 und SHA-512" konnte nicht aufgebaut werden.
- Wenn in der Konfiguration für eine IKEv2-Client-Verbindung kein IPv4-Adressen-Pool angelegt wurde, so erhielt der IKEv2-Client, welchem über den IKE-Config-Mode vom LANCOM Router eine IP-Adresse zugewiesen wurde, keinen DNS-Server. Der LANCOM Router weist dem IKEv2-Client als DNS-Server die eigene IP-Adresse zu, wenn kein IPv4-Adressen-Pool angelegt ist.
- Auf einer IKEv2-Verbindung, welche über IKEv2-RADIUS authentifiziert wurde, wurden nach mehr als 24 Stunden keine ausgehenden Daten mehr übertragen. Die Lifetimes wurden vom LANCOM Router in der RADIUS-Authentifizierung nicht korrekt übernommen.
- Bei einer für den LANCOM Advanced VPN Client angelegten IKEv2-Gegenstelle mit dem Verschlüsselungsverfahren AES-GCM wurden im aufgebauten VPN-Tunnel nur UDP- und ICMP-Pakete übertragen. TCP-Verbindungen funktionierten hingegen nicht (SSH, HTTPS etc.).
- Wenn in der Komandozeile eines LANCOM Routers der Befehl „show vpn" eingegeben wurde, zeigte die Ausgabe VPN-Regeln von konfigurierten IKEv2-Verbindungen als IKEv1-Regeln an.
- Wenn eine maskierte IKEv2-VPN-Verbindung zwischen zwei LANCOM Routern aufgebaut wurde, bei welcher auf einer Seite eine DMZ transparent (Maskierungs-Einstellung „nur Intranet") erreichbar sein sollte, so wurde auch die DMZ maskiert.
- Dynamic VPN-Verbindungen (IKEv1 über UDP) zwischen zwei LANCOM Routern, bei der die dynamische Seite mit einer privaten IP-Adresse auf der Internet-Verbindung (hinter einem NAT-Router) betrieben wurden, konnten nicht aufgebaut werden. Eine Dynamic VPN-Verbindung über ICMP funktionierte.

LCOS Änderungen von 10.12.0041 RC1 ▶ 10.12.0059 RC2

Neue Features

Allgemein

- Für den COM-Port-Server kann nun die Erreichbarkeit über WAN-Verbindungen konfiguriert werden.
- Dynamisch erzeugte VLAN-Mitgliedschaften können nun auf der CLI mit dem Befehl "show vlan" angezeigt werden.
- Die Dienstlisten der Layer-7-Anwendungserkennung wurden aktualisiert.
- Die Layer-7-Anwendungserkennung unterstützt nun die Erkennung von QUIC-Sessions.
- Unterstützung für Ethernet OAM nach 1TR112

WLAN

- Der Treiber für das IEEE 802.11ac Wave1-WLAN-Modul der folgenden Produkte wurde aktualisiert: LN-630acn dual Wireless, LN-822acn dual Wireless, LN-830acn dual Wireless, LN-830E Wireless, L-1310acn dual Wireless, L-1302acn dual Wireless, IAP-821, IAP-822, OAP-821, OAP-822, OAP-830

VoIP

- "Busy-on-Busy" ist nun für Rufgruppen konfigurierbar.

Korrekturen / Anpassungen

Allgemein

- Im Content Filter war die Kategorie "Cloud-Anwendungen" in den drei voreingestellten Default-Profilen als "Verboten" definiert. Dies wurde nun auf "Erlaubt" geändert.
- Die Uhrzeit, welche die LANCOM Management Cloud (LMC) periodisch setzt, wurde von einem LANCOM WLAN-Controller im Netzwerk überschrieben, wenn dieser seine Uhrzeit an einen von ihm verwalteten LANCOM Access Point meldete.
- In der Konfigurationsoberfläche des LANCOM 1783VAW fehlte die Möglichkeit zur Konfiguration der LACP-Schnittstellen "Bundle-1" und "Bundle-2".

VPN & Routing

- Wenn auf einem LANCOM Router VPN-Verbindungen terminiert wurden, die eine AES-GCM-Verschlüsselung verwendeten, so fehlten in der LCOS-Tabelle /Status/VPN/ESP die Werte in den Spalten "Crypt-Alg" und "Hash-Alg".
- Wenn auf einem LANCOM Router ausschließlich Default-Routen mit einem Routing-Tag ungleich 0 definiert waren, konnten IKEv2-Verbindungen nicht aufgebaut werden, wenn der IKEv2-Peer nicht anhand der IP-Adresse erkannt wurde.
- Es wurden weitere IPSec-Regeln generiert, wenn für eine VPN-Gegenstelle ausschließlich eine übergeordnete IPSec-Regel, zum Beispiel ANY-to-ANY, definiert war, aber auch für diese VPN-Gegenstelle ein oder mehrere N:N-NAT-Einträge hinterlegt waren, welche die übergeordnete IPSec-Regel einschloss.

WLAN

- Das Länderprofil „Australien“ wurde korrigiert.
- Bei Verwendung des Client-Bridge-Modus auf IEEE 802.11ac-fähigen WLAN-Modulen werden ARP-Pakete nun zuverlässig übertragen.
- Wenn im Menü Public-Spot -> Assistent > Bandbreitenprofile entsprechende Profile angelegt waren, wurden die Werte in der späteren Darstellung im Assistenten und auf dem Voucher vertauscht dargestellt.
- Das IEEE 802.11ac-Funkmodul eines LANCOM Access Point sendete im 2,4-GHz-Band sowohl im Modus 802.11gn/mixed als auch im Greenfield-Modus Beacons mit einer Datenrate von 1 MBit/s. Dies führte dazu, dass die Beacons auch auf einem 802.11b-Client sichtbar waren, obwohl der 802.11b-Modus in der Konfiguration des Access Points nicht ausgewählt war.
- Für die Public Spot-Loginmethode "Login nach Einverständniserklärung" wird nun auf der Statusseite kein Logout-Link mehr angezeigt.
- Auf der Login-Seite des Public Spot-Gateways konnte die Seite mit den Nutzungsbedingungen von Apple-Clients nicht aufgerufen werden, wenn das Authentifizierungsverfahren für den Public Spot auf "Anmeldedaten werden über E-Mail / SMS versendet" stand.
- Wenn in einem Public Spot-Szenario auf einem Router mit WLAN-Modul der Public Spot betrieben wurde und im lokalen Netz ein weiterer Access Point ebenfalls die Public Spot-SSID ausstrahlte, wurde der Eintrag für einen Client, der beim Roaming vom Router auf den Access Point wechselte, aus der Auto-Re-Login-Tabelle gelöscht. Dies führte dazu, dass ein erneutes Login am Public Spot erforderlich war.
- Bei einem LANCOM WLAN-Controller wurde nach Durchführung einer Funkfeldoptimierung im LANmonitor ein negativer Wert für verwaltete Access Points angezeigt.

VoIP

- Beim Betrieb einer VoIP-Leitung (SIP-Trunk) über einen BNG-Anschluss als Internetverbindung und Nutzung einer ISDN-TK-Anlage hinter einem LANCOM VoIP-Router konnte es gelegentlich zu einseitiger Sprachübertragung kommen. Der interne ISDN-Teilnehmer hörte den externen Teilnehmer nicht mehr.
- Telefonate von einer internen SIP-TK-Anlage über einen LANCOM VoIP Router an eine SIP-Trunk-Leitung des Providers "Deutsche Telefon" wurden nach ca. 15 Minuten getrennt.
- Wenn im Menü "Voice-Call-Manager --> Erweitert" ein oder mehrere Präfixe für interne Anrufe konfiguriert wurden, so wurde das konfigurierte Präfix bei der Quell-Rufnummer nicht angehängt. In der Folge konnte ein ausgehender Anruf nicht durchgeführt werden.
- Nach erfolgreicher Registrierung einer SIP-Leitung über IPv6 funktionierten eingehende Gespräche nicht, da die INVITE-Pakete von der Firewall des LANCOM VoIP-Routers mit einem "ICMP Port Unreachable" beantwortet wurden, obwohl eine vorhandene Inbound Firewall-Regel für den SIP-Server vorhanden war.

LCOS 10.12.0041 RC1

Geräte mit LCOS 10.12 RC1 können derzeit nicht über die LANCOM Management Cloud konfiguriert oder verwaltet werden.

Neue Features

Allgemein

- LACP - virtuelle Bündelung von Ethernet-Ports für hohe Ausfallsicherheit
- Public Spot-Unterstützung für den LANCOM vRouter
- Kommando zum Umschalten der Firmware mit anschließendem, automatischem Neustart
- Dateiimport per Copy & Paste
- Smart Ticket/SMS - Whitelist für Rufnummern-Vorwahlen
- Entfall des Ports 8080 bei WEBconfig und Public Spot
- Erweiterung des Content-Filters um weitere Kategorien
- IPv6-Unterstützung für den Content-Filter

VPN & Routing

- IKEv2 Load Balancer für das Load Balancing eingehender VPN-Verbindungen
- Frei konfigurierbare DHCPv6-Optionen
- OSPFv2
- OCSP-Prüfung im TLS/Rollout-Agent
- Schaltbare Nicht-HTTPS-Kommunikation über Port 443 im Content-Filter
- Unterstützung von AES-GCM bei IKEv2
- Unterstützung der elliptischen Diffie-Hellmann-Gruppen (ECDH) 19, 20 und 21 sowie der ECC Brainpool-Kurven 28, 29 und 30 bei IKEv2
- Unterstützung für RADIUS CoA bei IKEv2
- Erweiterte VPN-Backup-Mechanismen für höchste Verfügbarkeit im VPN
- Unterstützung für TACACS Shell-Autorisierung
- Variablen für IPv6-LAN-Adresse und Präfix in der Aktionstabelle
- ICMPv4 und ICMPv6-Rate-Limiting
- Unterstützung von MD5 im NTP-Client und Server
- NTP-Server pro ARF-Netz schaltbar

WLAN

- Multicast > Unicast-Umwandlung für ruckelfreies IPTV im WLAN
- Die Menüs zur Public Spot-Konfiguration sind ab sofort grundsätzlich im LCOS vorhanden, können aber erst nach erfolgreicher Aktivierung der Public Spot-Option verwendet werden.
- Erreichbarkeitsprüfung für RADIUS-Server im 802.1X
- 802.11ac Wave 2 Features via WLC konfigurierbar
- Koordinierte Wireless ePaper-Kanalwahl

VoIP

- Das SIP User-ID-Feld ist nun schaltbar
- Overlap Dialing ermöglicht schnelleren Verbindungsaufbau

Korrekturen / Anpassungen

Allgemein

- Wenn die Gültigkeit eines RA-Zertifikates vor der Gültigkeit des CA-Zertifikats ablief, aktualisierte der SCEP-Client das RA-Zertifikat nicht.
- Wenn die Spanning Tree-Funktion per LANconfig auf LANCOM Access Points aktiviert wurde, wurde diese Änderung nicht korrekt zurückgeschrieben, sodass Spanning Tree nach dem Zurückschreiben der Konfiguration weiterhin deaktiviert war.
- Beim Hochladen einer vRouter-Konfiguration per WEBconfig wurden die Konfigurationsparameter nur dann vollständig übernommen, wenn beim vRouter nach dem Hochladen der Konfiguration ein Warmstart ausgeführt wurde.
- Bei Verwendung eines Backup RADIUS-Servers zur Geräte-Authentifizierung wurde das Login zuerst auf dem Backup-Server statt auf dem primären RADIUS-Server geprüft.
- Wenn in der Zeit des DHCP-Bezugs der DHCP-Client neu startete, konnte es vorkommen, dass der LANCOM DHCP-Server diesem Client nach dem Neustart keine IP-Adresse mehr zuwies, und in der Trace-Ausgabe zu DHCP die Meldung "ARP in progress" erschien.
- Proxy-ARP für die Kommunikation zwischen identischen, vom LANCOM verwalteten IP-Netzwerken wurde nicht ausgeführt.
- Bei einer Internet-Verbindung, die als DS-Lite angelegt war, konnte es vorkommen, dass der LANCOM für IPv6-Pakete nicht seine IPv6-WAN-Adresse, sondern seine IPv6-LAN-Adresse als Absender verwendete.
- Der LCOS CRL-Client fragte alle Typen von CRL-Distribution-Points ab, obwohl der CRL-Client nur den Typ HTTP unterstützt.
- Die Tabelle "Setup/DNS/DNS-Destinations" (LANconfig: IPv4 -> DNS -> Weiterleitungen) akzeptierte für den Parameter "Rtg-tag" (Routing-Tag) nur Werte kleiner oder gleich 999.
- Im LANCOM vRouter fehlten im Setupmenü "/Setup/WAN" die Tabellen zur Konfiguration von Backup und Accounting.
- Wenn auf der Kommandozeile der Befehl "show script" eingegeben wurde, enthielt die Ausgabe keine Session-IDs mehr. Laufende Skripte konnten daher nicht mehr mit dem Befehl "killscript <Session-ID>" gestoppt werden.
- Im LANCOM vRouter fehlte das Setupmenü (/Setup/WAN/RADIUS) für die Authentifizierung über einen externen RADIUS-Server.
- Eine xDSL-Verbindung wurde nicht sofort abgebaut, wenn die dazugehörige DSL-Gegenstelle per Script aus der Konfiguration gelöst wurde.
- Es konnte zu einem unvermittelten Neustart des Gerätes nach Aufruf des benutzerdefinierten Rollout-Assistenten kommen, wenn im benutzerdefinierten Rollout-Assistenten für eine Auswahl-Liste mehr Werte (item_value) als Text (item_text) definiert waren.

VPN

- Sollte eine DHCP-Anfrage über einen VPN-Tunnel weitergeleitet werden, der über den Config-Mode eine IP-Adresse erhielt, wurde die Config-Mode Adresse auch als GI-Adresse im DHCP-Header eingetragen.
- Wenn eine bestehende VPN-Verbindung mit einer Delete-Information abgebaut wurde, war im VPN-Debug-Trace keine Information über den Auslösegrund enthalten.
- Im WEBconfig-Konfigurationsdialog für die IKEv2-Rekeying-Parameter (Konfiguration -> VPN -> IKEv2/IPSec -> Gültigkeitsdauer) fehlten Namensbezeichnungen bei zwei konfigurierbaren Parametern.
- Wurde eine IKE-Verbindung, die zwischen einem vRouter und einem VPN-Router aufgebaut werden sollte, per DPD überwacht, erfolgte immer wieder ein Verbindungsabbruch auf Grund eines DPD Timeout. Das DPD wurde auf dem LANCOM vRouter nicht korrekt ausgeführt.

WLAN

- Der Trigger zur Re-Initialisierung des SCEP-Clients konnte ins Leere laufen, wenn sich der Client gerade in der Initialisierung befand.
- Der Wert zur Begrenzung des Datenvolumens für automatisch erzeugte Public-Spot Benutzer im Pfad "/Setup/Public-Spot-Module/Authentication-Modules/User-Template/Volume-Budget" war auf einen Maximalwert von 4.000 MByte begrenzt.
- Beim Erstellen von Public-Spot-Benutzern per HTTP-Befehl wurde ein in der URL angegebener Kommentar nicht in das erstellte Benutzerprofil übernommen.
- Es konnte zu einem unvermittelten Neustart des Gerätes kommen, wenn der Access Point für die WLAN-Clients einen WLC-Tunnel (CAPWAP-Datentunnel) bereitstellte und einem WLAN-Client ein ICMP-Paket "Fragmentation needed" zustellen wollte, da das vom WLAN-Client empfangene Datenpaket zu groß für den CAPWAP-Datentunnel war.

VoIP

- Wenn ein Anruf über eine ISDN-TK-Anlage erfolgte, die an der internen ISDN-Schnittstelle des LANCOM Routers angeschlossen ist und über eine konfigurierte Rufweiterleitung an externe Nummern verfügt, führte dies zu einer unidirektionalen Kommunikation, wenn der Ruf schließlich über den VCM per SIP zum Provider weitergeleitet wurde.
- Bei einem ausgehenden SIP-Anruf wandelte der LANCOM Voice Call Manager eine Landesvorwahl, welche mit einem "+" beginnt (z.B. +492405123456) nicht in das Format 0049 um, was zur Folge hatte, dass eine ISDN-Telefonanlage die Rufnummer nicht auswerten und der Anruf nicht durchgeführt werden konnte.
- Wenn auf der Konsole die SIP-Leitung mit dem Befehl "do /other/manual-dialing/disconnect <Verbindung>" getrennt wurde, dann wurde der LANCOM Voice Call Manager nicht über das Trennen der Verbindung informiert, was zur Folge hatte, das die Leitungen, die diese 'Verbindung' nutzen, nach wie vor als registriert angezeigt wurden.
- Abgehende Telefonate über den SIP-Provider M-net konnten nicht aufgebaut werden, da der Provider sowohl nach der Authentifizierung über ein "INVITE" als auch nach einem "PRACK" eine Authentifizierung fordert.
- Wenn ein VoIP-Provider auf die De-Registrierung einer SIP-Leitung mit der Fehlermeldung "400 Bad Request" antwortete, konnte der LANCOM Voice Call Manager diese Fehlermeldung nicht interpretieren, was dazu führte, dass die De-Registrierung der SIP-Leitung ständig wiederholt wurde und keine Neuregistrierung stattfinden konnte.
- Sollte eine Rufgruppe als Backup-Leitung, z.B. für eine Verbindung zu einer TK-Anlage, verwendet werden, so funktionierte dieser Eintrag nicht.
- Eine SIP-Session, welche über eine Firewall-Regel mit einen Routing-Tag versehen wurde und dann durch den SIP-ALG gemanagt wurde, konnte nicht aufgebaut werden, da die Antwort-Pakete mit dem gleichen Tag (Quell-Tag) vom SIP-ALG versehen, und so vom IP-Router verworfen wurden.
- Eine SIP-Leitung, welche mittels OPTIONS-Pakete registriert wurde, wurde vom SIP-ALG nicht als registrierte Leitung interpretiert, demzufolge eingehende Calls (INVITE-Pakete) nicht korrekt zugeordnet wurden.
- Aufgrund des Parameters "transport=UDP" im Contact-Header eines SIP-Paketes verloren einige lokale SIP-Clients nach wenigen Minuten die Registrierung zum LANCOM VoIP-Router.
- Bei LANCOM VoIP-Routern trat ein sporadisches Problem bei Anrufen auf, an denen die LANCOM 510 DECT Basisstation beteiligt war. Wenn ein externer Ruf auf einer SIP-Leitung am LANCOM VoIP-Router ankam und intern an einem Handset des LANCOM N510 DECT angenommen wurde, hörte der Anrufer den internen Teilnehmer, der interne Teilnehmer aber den Anrufer nicht.
- Es konnte zu einem unvermittelten Neustart des Gerätes kommen, wenn das empfangene OK-Paket auf einer SIP-Leitung im CONTACT-Header keinen Expires-Wert beinhaltete.
- Es konnte sporadisch eine einseitige Verständigung auftreten, wenn ein eingehender Call über eine SIP-Leitung vom LANCOM VoIP-Router intern auf mehr als 2 Interfaces (ISDN- und Analog-Schnittstellen) signalisiert wurde.

- Ein SETUP, welches auf dem ISDN empfangen wurde und eine Zielrufnummer vom Typ "National Number" enthielt, wurde vom Call-Routing nicht um Nullen ergänzt, wie es z.B. bei Nummern vom Typ "International Number" der Fall ist. In der Folge scheiterte das Call-Routing mit Service-Nummern.
- Nachdem ein analoger Anruf beendet wurde, blieb dieser in seltenen Fällen in der Call Counter-Tabelle des LANCOM VoIP-Routers als Eintrag erhalten.
- Ein Linphone SIP-Client wurde bei der Anmeldung am Voice Call Manager (VCM) aufgrund von für den Client spezifischen Parametern innerhalb der Anmeldung abgelehnt.

3. Wichtige Hinweise

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 erst nach einem internen Test in der Kundenumgebung aktualisiert werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

Hinweise

- 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 https://www.lancom-systems.de/produkte/lcos/lifecycle-management/produkttabellen/

Gerätespezifische Empfehlungen

LANCOM 178x-4G:
Um Verzögerungen beim Aufbau von Mobilfunk-Verbindungen (z.B. im Backup-Fall) zu vermeiden, wird empfohlen, im verbauten LTE-Mobilfunk Modem des Typs Sierra MC-7710 **den LTE-Modem-Treiber der Version 3.5.24 einzusetzen**. Beachten Sie dazu bitte auch den folgenden Knowledge Base-Artikel: Link

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.

Verwendung von Dynamic VPN

Aus patentrechtlichen Gründen muss die Verwendung der Funktion „Dynamic VPN“ mit Übertragung der IP-Adressen über den ISDN-Anschluss lizenziert werden. Diese Betriebsart kommt in der Regel dann zum Einsatz, wenn Sie VPN-Kopplungen mit beidseitig dynamischen IP-Adressen nutzen und dabei keine Dynamic-DNS-Dienste verwenden.

Alle anderen Betriebsarten von Dynamic VPN (die Übermittlung der IP Adresse per ICMP, das Anklopfen bei der Gegenstelle per ISDN, um einen Rückruf herbeizuführen etc.) sind davon nicht betroffen.

Die Registrierung erfolgt anonym über das Internet, es werden keine personen- oder unternehmensspezifischen Daten übertragen.

Zur Registrierung der “Dynamic VPN” Option benötigen Sie Administratorrechte auf dem LANCOM-Router.