Release Notes

LCOS SX

3.34 RU7

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.

LCOS SX 3.32 / 3.34 ist das Betriebssystem für alle LANCOM Switches der GS-1300- / GS-2300-Serie.

Für alle LANCOM Switches der XS-Serie steht das Betriebssystem LCOS SX 5.x zur Verfügung.
Für alle LANCOM Switches der Serie GS-3xxx steht das Betriebssystem LCOS 4.x zur Verfügung.
Die Release Notes zu diesen Geräteserien finden Sie wie gewohnt auf der LANCOM Webseite im Downloadbereich des jeweiligen Switches.

Dieses Dokument beschreibt die Neuerungen der LCOS SX Software Release 3.34 RU7 sowie die Änderungen und Verbesserungen zur Vorversion.

Bitte **sichern Sie** vor dem Update Ihrer LANCOM-Geräte auf eine neue Firmware-Version **unbedingt Ihre Konfigurationsdateien!**
Aufgrund der teils umfangreichen Feature-Erweiterungen ist ohne eine solche Sicherung ein **Downgrade** auf die alte Firmware **nicht mehr automatisch möglich**.
Bitte beachten Sie, dass für Ihr Gerät unterschiedliche Firmware-Dateien zur Verfügung stehen können.

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. Hinweis zum Firmware-Update

Trennen Sie den Switch während eines Firmware-Updates niemals vom Stromnetz, da das Gerät bei einem Abbruch des Aktualisierungsvorganges nicht mehr ordnungsgemäß startet.

Bitte **sichern Sie** vor dem Update Ihrer LANCOM-Geräte auf eine neue Firmware-Version **unbedingt Ihre Konfigurationsdateien!**
Aufgrund der teils umfangreichen Feature-Erweiterungen ist ohne eine solche Sicherung ein **Downgrade** auf die alte Firmware **nicht mehr automatisch möglich**.
Bitte beachten Sie, dass für Ihr Gerät unterschiedliche Firmware-Dateien zur Verfügung stehen können.

4. Neue Features, Änderungen und Historie

Nur LANCOM GS-2300-Serie:

Geräte, die mit LCOS SX 3.30 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 jederzeit auf der WEBconfig-Oberfläche unter Konfiguration > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0324 RU7

→ Bei mehreren Chargen von GS-2326P+ mit Herstellungsdatum 24.01.2024 und 31.01.2024 meldete der Switch bereits bei geringer PoE-Auslastung, dass die maximale PoE-Leistung erreicht war. Dies führte dazu, dass nur sehr wenige Geräte per PoE mit Strom versorgt werden konnten. Im ‘Port-Status’ der nicht funktionierenden Ports wurde dann entweder die Meldung “PoE Overload” oder “PoE disabled” ausgegeben.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0323 RU6

Korrekturen / Anpassungen

→ Bei einem durch die LMC verwalteten Switch mit LCOS SX 3.34 RU5 und einer statischen IP-Adresse konnte dieser nach einem Rollout nicht mehr die LMC kontaktieren.

→ Im Zuge der Behebung der ‚Terrapin'-Sicherheitslücke wurde der ‚strict-kex'-Modus eingeführt. Statt diesen Modus für jede SSH-Verbindung einzeln auszuhandeln, verwendete der Switch diesen für alle Verbindungen. Dies führte dazu, dass die Verschlüsselungs-Aushandlung für Gegenstellen ohne ‚strict-kex'-Unterstützung nicht mehr möglich war und somit die SSH-Sessions nicht aufgebaut werden konnten.

→ Nach einem Update auf LCOS SX 3.34 RU5 konnte es vorkommen, dass der Switch einen SSH-Schlüssel mit falscher Größe generierte. Dies führte dazu, dass sich der SSH-Dienst beendete und der Switch einfror.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0320 RU5

Korrekturen / Anpassungen

→ Nach einer Firmware-Aktualisierung wurden die Informationen von eingesteckten SFP-Modulen nicht mehr in der Konfiguration angezeigt.

→ Das Maximum für die Verarbeitung von 802.1X-Identitäten lag bei 39 Zeichen. Dieses Maximum wurde nun auf 253 Zeichen erhöht.

→ Es konnte vorkommen, dass ein Switch bei einem Zugriff per SSH einen unvermittelten Neustart durchführte.

→ Nach drei fehlgeschlagenen ‚Auto Negotiations' wurde die Port-Geschwindigkeit vom Switch durch eine Downshift-Funktion auf max. 100 MBit/s eingestellt (Standardeinstellung). Dies führte in einigen Szenarien dazu, dass ausgehandelte schnellere Port-Geschwindigkeiten auf 100 MBit/s zurückfielen, wenn z.B. ein Client im Standby-Modus war. Die Downshift-Funktion kann nun mit dem Befehl ‚downshift <port-list> disable' deaktiviert werden.

→ Nach einem ‚DHCP Renew' trennte der Switch alle HTTP-Verbindungen. In einem LMC-Szenario wurde dadurch auch die Verbindung zum LMC-Monitoring getrennt, was zu einem unvermittelten Neustart des Switches führte.

→ In Einzelfällen konnte es in einem LMC-Szenario vorkommen, dass der Switch keine Monitoring-Daten an die LMC sendete.

→ Bei gleichzeitiger Verwendung des Tagging-Modus Hybrid sowie ‚Port-based 802.1X' auf einem Port lernte der Switch die MAC-Adressen der über den Port angebundenen Geräte nur für das VLAN 1 (untagged VLAN). Wechselte ein angebundenes Gerät in einem tagged VLAN auf einen anderen per ‚Port-based 802.1X' abgesicherten Port (etwa durch Roaming auf einen anderen Access Point), konnte der Switch die MAC-Adresse nicht korrekt dem neuen Port zuweisen. Dadurch funktionierte die Kommunikation in dem tagged VLAN nach einem Wechsel des Ports nicht mehr.

→ Eine im WEBconfig durchgeführte Abfrage nach existierenden Benutzerprofilen lieferte neben allgemeinen Benutzerdaten auch das Passwort im Klartext. Das Passwort wird nun nicht mehr mitgesendet.

→ Die Verwendung von CBC-Verschlüsselungs-Algorithmen wurde deaktiviert, was zur Folge hat, dass auch alle 3DES-Verschlüsselungsvarianten deaktiviert wurden.

→ Die Verwendung der Hash-Algorithmen
- diffie-hellman-group14-sha1,
- diffie-hellman-group1-sha1,
- hmac-sha1-96,
- hmac-sha1

wurde deaktiviert.

→ Nach dem Login eines Benutzers im Webinterface wird ein Session-Cookie gesetzt. Dieses enthielt fälschlicherweise die Login-Daten des Benutzers (Base64-kodiert).

→ Der SSH-Dienst Dropbear wurde aktualisiert. In der neuen Version wurden veraltete Algorithmen deaktiviert und Sicherheitspatches eingepflegt.
- Die Unterstützung für den Algorithmus DSA (SSH-DSS) wurde entfernt.
- Die Unterstützung für die Diffie-Hellman-Gruppe 1 wurde entfernt.
- Die Unterstützung für SSH-RSA (SHA1) wurde entfernt und durch SSH-RSA-SHA2-256 abgelöst.

→ Die lokale Benutzerdatenbank verwendet jetzt den Hash-Algorithmus Argon2.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0205 RU4

Neue Features

→ Erweiterung des Radius Supplicant-Features um einen Schalter, der die vom 802.1X Supplicant verwendete MAC-Adresse auf die System-MAC-Adresse ändert. Dies vereinfacht die Nutzung der Single- und Multi-Auth-Modi.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0204 RU3

Neue Features

→ Der LMC CLI- und WebGUI-Tunnel wurde analog zu den anderen Switch-Serien hinzugefügt.

→ Der Switch kann nun als ‚Supplicant' am RADIUS-Server authentifiziert werden.

→ SYSLOG-Unterstützung nach RFC-5424 wurde eingebaut.

→ SYSLOG-Meldungen beinhalten nun den Hostnamen statt der IP-Adresse.

→ Access Control List-Einträge lassen sich jetzt per CLI-Befehl <delete all> im ACL-Menü vollständig löschen.

Korrekturen / Anpassungen

→ Der Fallback von einer 802.1X-Authentifizierung auf eine MAC-basierte Authentifizierung schlug fehl, wenn der Client die EAP-Anfragen mit ‚EAP logoff'-Paketen beantwortete, um die 802.1X-Authentifizierung abzulehnen.

→ Wenn über die Kommandozeile des Switches eine ACL-Regel (Access Control List) für IPv4 mit dem Frame Type ‚255.255.255.255/32' angelegt wurde, so wurde dieser Wert nicht akzeptiert.

→ In Syslog-Meldungen wurde statt des Host-Namens die IP-Adresse angezeigt, was die genaue Identifizierung des Gerätes erschweren konnte. Es wird jetzt der Host-Name angezeigt.

→ Wenn ein LANCOM GS-2310x sich als RADIUS Supplicant über seine MAC-Adresse an einem RADIUS-Server authentifizieren sollte und der Switch über einen der Combo-Ports angebunden wurde, zählte der Switch die MAC-Adresse auf den Combo-Ports hoch. Dies führte dazu, dass dem RADIUS-Server eine falsche MAC-Adresse gemeldet wurde und die Authentifizierung fehlschlug.

→ Ein Login über einen CLI-Tunnel erzeugte keinen Eintrag im Syslog des Switches.
→ In Szenarien, in denen der Switch als Authenticator eingesetzt wurde, enthielt das RADIUS-Paket nach einem Neustart des Switches keine IP-Adresse im ‚NAS'-Feld. In der Folge erhielten die authentifizierten Clients keine IP-Adresse.
→ Die automatische Aktualiserung der Konfigurationsoberfläche war funktionslos und konnte nach einer Aktivierung nicht mehr deaktiviert werden.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0101 RU2

Neue Features

→ RADIUS MAC address Bypass / Fallback wurde hinzugefügt - wird z. B. die 802.1X-Authentifizierung abgelehnt, wird nach einer optional definierbaren Wartezeit die MAC-based-Anfrage gesendet.
→ RADIUS assigned VLANs werden jetzt auch für die Multi-Client-Modi ‚Multi 802.1X' unterstützt.

Korrekturen / Anpassungen

→ Die Port-Konfiguration einer ‚Mac-based Single' Client-Authentifizierung in Verbindung mit Port Security konnte zu einer endlosen Bootschleife des Switches führen, welche nur durch Ziehen des Verbindungskabels zum Client wieder behoben werden konnte.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0006 RU1

Korrekturen / Anpassungen

→ Nach einem Neustart leitete der Switch kurzzeitig die VLAN-Tags nicht weiter. Dadurch konnte es vorkommen, dass Netzwerk-Teilnehmern, welche an einem ‚Access'-Port angeschlossen waren, per DHCP kurzzeitig eine IP-Adresse aus dem untagged Management-Netzwerk zugewiesen wurde. Erst nach Ablauf des DHCP-Leases wurde dann eine IP-Adresse aus dem korrekten Netzwerk zugewiesen.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.34.0003 Rel

Neue Features

→ Das Spanning Tree Protocol (STP) lässt sich jetzt aus der LMC heraus konfigurieren.

→ Aus dem Debug Menü lassen sich das persistente Event- und Bootlog löschen (debug; erase persistent-logs).

→ Bei der IP-Source-Guard-Konfiguration sorgt ein ‚Mouseover' in der Beschreibungs-Spalte für komfortable Port-Detail-Informationen.

Korrekturen / Anpassungen

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

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

→ Bei Verwendung von 802.1X mit dem Authentifizierungs-Modus ‚MAC-based Auth.' konnte die Funktion ‚RADIUS-Assigned VLAN Enabled' nicht aktiviert werden.
Es wurde ein neuer Authentifizierungs-Modus ‚MAC-based single Auth.' implementiert, mit dem die Verwendung der Funktion ‚RADIUS-Assigned VLAN Enabled' möglich ist.

→ Wenn in der Konfiguration für die Zeitumstellung (MEZ/MESZ) ein Sonntag als Zeitumstellungs-Tag angegeben war, zeigte der Switch nach der Zeitumstellung eine falsche Uhrzeit an, wenn ein NTP-Zeitserver als ‚Clock Source' eingestellt war.

→ Der OID-Wert ‚Serial' wurde in Monitoring-Tools mit dem falschen Wert ‚System MAC: <MAC-Adresse>' ausgegeben.

→ Bei der Übermittlung von LLDP-Daten fehlte im Wert ‚Management Address IPv4' die IP-Adresse. Dort war stets die Adresse 0.0.0.0 eingetragen.

→ Bei der Angabe der Firmware-Informationen in der LMC im Menü ‚Geräte / <Gerätename> / System-Informationen' übermittelte der Switch lediglich die Versionsangabe. Die Datumsangabe hinter der Versionsnummer fehlte jedoch.

→ Bei einer Firmware-Aktualisierung auf LCOS SX 3.34 Rel werden in der Konfiguration des Switches automatisch neue RSA SSH-Hostkeys erzeugt.

→ Bei der Verwendung von Protokollen mit portgebundenen Paketen (z.B. STP oder LLDP) verwendete ein Switch der GS-2300-Serie seine Management-MAC-Adresse statt einer eigenen MAC-Adresse je Port.

→ Wenn die Syntax in der Switch-Konfiguration nicht korrekt angegeben und die Konfiguration in den Switch hochgeladen wurde, konnte dies zu einem unvermittelten Neustart des Switches führen. Eine Fehlermeldung wurde in diesem Fall nicht ausgegeben.

→ Beim Import einer Switch-Konfiguration wird diese zuerst auf Syntax-Fehler überprüft und anschließend eingelesen. Der PoE-Baum wurde aber direkt eingelesen ohne eine Syntax-Prüfung durchzuführen. Dies konnte zu einer fehlerhaften PoE-Konfiguration führen.

→ Ein Scan mit einem Vulnerability Scanner konnte zu Abstürzen einzelner Prozesse eines SSH-Dienstes führen. Der Switch konnte anschließend nicht mehr per SSH erreicht werden.

→ Bei Verwendung von DHCP-Snooping und gleichzeitiger Konfiguration von LACP oder Spanning Tree auf den ‚Trusted Ports' wurden DHCP-Pakete auf allen ‚Trusted Ports' versendet und somit dupliziert bzw. sogar vervielfacht. Dies konnte zu ‚DHCP flooding' im Netzwerk führen.

→ Einzelne Funktionen setzen für die Bearbeitung bestimmte Berechtigungen voraus (‚Privilege Level'). Die Einstellungen für die Funktion ‚Easyport' konnten nicht mit einem Benutzer mit dem ‚Privilege Level' 12 bearbeitet werden, sondern nur mit einem Benutzer mit dem Level 15. Weiterhin war für die Konfiguration der Funktion ‚LLDP-MED' ein Benutzer mit dem Privilege Level 6 (gleiches Level wie die Funktion ‚LLDP') erforderlich statt mit dem Privilege Level 5.

→ Bei Verwendung der DHCP-Option 43 im Netzwerk mit einer ‚Value Size' größer als 127 Bytes konnte der Switch die DHCP-Pakete nicht korrekt verarbeiten und daher keine IP-Adresse per DHCP beziehen.
DHCP-Pakete mit der Option 43 können jetzt bis zu einer Größe von 255 Bytes verarbeitet werden.

→ Wenn während einer Firmware-Aktualisierung Konfigurationsänderungen per WEBconfig oder Kommandozeile durchgeführt wurden, startete der Switch nach der Aktualisierung mit der neuen Firmware, jedoch ohne die geänderte Konfiguration. Es ist nun nicht mehr möglich, Konfigurationsänderungen während der Firmware-Aktualisierung durchzuführen.

→ In der Konfiguration eines Switch-Namens wurde einem beliebig konfigurierten Namen stets das Prefix „LANCOM-" vorangestellt.

→ Wenn an einem Switch-Port eine Single-Authentifizierung mit aktivem Gast-VLAN konfiguriert wurde, legte der Switch die Clients ohne Authentifizierung laut MAC-Tabelle in das entsprechende VLAN für das Gast-Netzwerk, die Clients erhielten jedoch keine IP-Adresse per DHCP.

→ Wenn mehrere Clients auf einem 802.1X-Multi-Client Port verbunden sind, bestimmt der letzte gesehene Client, ob Broadcasts auf dem Port möglich sind. Wenn jedoch zuletzt ein Client gesehen wurde, welcher nicht auf dem Port zugelassen war, schaltete der Switch die Broadcasts auf dem Port ab.
→ In der RADIUS-Server-Tabelle konnte im Feld ‚Hostname' lediglich eine IP-Adresse eingetragen werden.

Nur GS-2300-Serie:

→ Wenn bei den Switches der GS-2300-Serie ein Passwort mit 32 Zeichen konfiguriert wurde, konnte man sich mit diesem Passwort nicht mehr am WEBconfig des Switches anmelden. In der LMC sorgte ein Passwort mit 32 Zeichen dafür, dass beim Aufruf der Detailkonfiguration eine Fehlermeldung eingeblendet wurde und die Detailkonfiguration nicht mehr verwendet werden konnte.
→ Mit dem Konsolen-Befehl ‚startlmc' kann im LCOS ein Pairing mit der LMC unter Angabe der Seriennummer sowie des Cloud-Pins vorgenommen werden. Bei Ausführung des Befehls ‚startlmc' auf LCOS SX wurde fälschlicherweise zusätzlich noch ein Aktivierungscode aus der LMC angefordert.
→ Bei der sFlow-Funktion sendete der Switch bei aktivierter Mode-Option (Status: enabled) ausschließlich ‚Counters sample'-Pakete und keine ‚Flow sample'-Pakete. In der Folge konnten Informationslücken bei der Überwachung der Geräte mit Monitoring-Tools anderer Hersteller (z.B. PRT) auftreten.
→ Es konnte vereinzelt vorkommen, dass der Pairing-Vorgang eines Switches mit der LMC oder der Ausroll-Vorgang einer Konfiguration durch die LMC auf den Switch aufgrund eines fehlerhaften Parameters fehlschlug, obwohl dieser Parameter auf dem Switch nicht konfiguriert wurde. In der LMC wurde in diesem Fall die Fehlermeldung „Nicht akzeptiert" ausgegeben.
→ Ab LCOS SX 3.32 RU7 wird für Authentication-Requests an Switch-Ports der Service-Type ‚Call-Check' verwendet.
Gemäß Best Practice in RFC 3580 wird jetzt für ‚802.1X' requests der Service-Type ‚Framed' und für ‚MAC-based' requests der Service-Type ‚Call-Check' verwendet.
→ Bei den Switches der LANCOM GS-2300-Serie ist das Telnet-Protokoll im Werkszustand nun standardmäßig deaktiviert.
→ In der Konfiguration der Swich-Ports ist es jetzt möglich, dass ein Voice-VLAN und eine MAC-basierte Authentifizierung über einen Port an Clients in zwei verschiedenen VLANs geleitet werden.

→ Das Bootlog sowie das Eventlog konnten nicht gelöscht werden. Dies konnte dazu führen, dass die Logs sehr groß wurden und nur langsam geladen werden konnten.
Die Logs können jetzt auf der Konsole im Debug-Menü (debug) mit dem Befehl ‚erase persistent-logs' gelöscht werden.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0222 RU7

Korrekturen / Anpassungen

→ Bei einer MAC-based 802.1X-Authentifizierung gegen einen RADIUS-Server wurde ein Client authentifiziert, obwohl die RADIUS-Authentifizierung mit einem ‚RADIUS Reject' und ‚EAP Success' beantwortet wurde. Das EAP-Paket vom Typ ‚Success' bezieht sich jedoch nur auf die erfolgreiche EAP-Kommunikation.

→ Der Switch interpretierte nur den EAP-Teil, aber nicht den Inhalt des RADIUS-Pakets (das ‚RADIUS Reject'). Deshalb wurde ein Client, welcher nicht auf dem RADIUS-Server bekannt war, ebenfalls erfolgreich authentifiziert.

→ Der Switch ist jetzt in der Lage, die RADIUS-Attribute ‚NAS Identifier' und ‚Service Type=Call Check' zu übermitteln.

→ Die maximale Länge eines SSH-Hostkey wurde von 1024 Bit auf 2048 Bit erweitert.

→ Eine MAC-based 802.1X-Authentifizierung gegen einen RADIUS-Server wurde als RADIUS-Request ohne EAP-Bestandteile und mit der MAC-Adresse als Benutzername übergeben.

→ Bei Verwendung einer 802.1X-Authentifizierung mit den Modi ‚Single 802.1X,' ‚Multi 802.1X' und ‚MAC-based Auth.' wurden nach dem erfolgreichem Login der Endgeräte die MAC-Adressen nicht in die MAC-Adress-Tabelle übernommen.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0221 SU6

Korrekturen / Anpassungen

→ Spezielle Benutzereingaben über das Webinterface wurden nicht korrekt validiert. Dadurch konnte ein unvermittelter Neustart des Gerätes provoziert werden.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0210 RU5

Korrekturen / Anpassungen

→ Beim Betrieb von LANCOM Switches der GS-1300- / GS-2300-Serie konnte es vorkommen, dass Geräte nach einem Neustart ihre Seriennummer und MAC-Adresse verloren und auch keine IP-Adresse mehr beziehen konnten. Der Betrieb der Geräte war weiterhin gegeben, die betroffenen Switches konnten jedoch nicht mehr über ihre IP-Adresse erreicht werden.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0208 RU4

Neue Features

→ In der ‚Authentication Method Configuration' besteht nun die Möglichkeit, die Protokolle HTTP und HTTPS getrennt zu konfigurieren.

→ Vereinfachung der VLAN-Portmarkierung

→ In der ‚System Log Configuration' wird nun eine Warnung bei unsicherer ‚SNMPv2 Get community'-Konfiguration angezeigt.

Korrekturen / Anpassungen

→ Die in den Kofigurationsdateien hinterlegten Passwörter werden nun verschlüsselt abgespeichert.

→ Bei Verwendung von 802.1X mit dem Authentifizierungs-Modus ‚Mac-based Auth.' konnte die Funktion ‚RADIUS-Assigned VLAN Enabled' nicht aktiviert werden.

→ Es wurde ein neuer Authentifizierungs-Modus ‚MAC-based single Auth.' implementiert, mit dem die Verwendung der Funktion ‚RADIUS-Assigned VLAN Enabled' möglich ist.

→ Obwohl der Zugriff auf das Webinterface in der Konfiguration gesperrt war, wurde bei einem Zugriffsversuch die Login-Seite des Webinterfaces angezeigt. Ein Login war jedoch nicht möglich.

→ Nach Deaktivierung von ‚Web' in der ‚Authentication Method Configuration' wurde der Port 80 als offen angezeigt, ein Zugriff auf die Web-Oberfläche war jedoch nicht möglich.

→ Bei Verwendung des Features ‚Port Based 802.1X' und dem VLAN-Modus ‚Trunk' konnte ein angeschlossenes Gerät zwar authentifiziert werden, eine Datenübertragung war aber nicht möglich.

→ Wurde auf dem Switch ein Voice VLAN konfiguriert, war sporadisch die MAC-Adresse von einzelnen angeschlossenen Netzwerk-Geräten nach dem Ablauf der ‚Voice VLAN Aging Time' nicht mehr in der MAC-Address-Tabelle enthalten. Dadurch konnten diese Geräte nicht mehr im Netzwerk kommunizieren. Es waren nur Geräte in VLANs betroffen, die nicht dem Voice VLAN entsprachen.

→ Beim Setzen eines statischen MAC-Tabellen-Eintrags im Menü ‚Filtering Data Base / Configuration' startete der Switch unvermittelt neu

→ Wurde ein Port-basiertes VLAN konfiguriert und zusätzlich eine Konfiguration für MAC-basiertes VLAN hinzugefügt, funktionierten nur noch die MAC-basierten Einstellungen; die weitergehenden Einstellungen wurden ignoriert.

→ Die Funktion ‚Limit Control' im Menü ‚Security / Port Security' konnte nur über die Web-Oberfläche aktiviert werden. Wurde versucht, die Funktion über die Konsole zu aktivieren, wurde die Fehlermeldung „Port Security Limit Control Configuration of easyport must be preserved" ausgegeben.

→ **Nur GS-2300-Serie:** In der SNMP-MIB eines LANCOM GS-2310(P)(+) wurden bei aktivem LACP im Baum LLDP 13 Ports ausgegeben, obwohl der Switch nur über 12 Ports verfügt.

→ **Nur GS-2300-Serie:** Das (Admin)-Passwort, der User-Name und der Privilege Level ließen sich nicht per SNMP mit dem bereits vorhandenen Admin-Account konfigurieren.

→ **Nur GS-2300-Serie:** Auf der Konsole gab es keine Möglichkeit, mehrere Protokolle für den Zugriff auf den Switch gleichzeitig zu aktivieren (z.B. SNMP & TELNET/SSH). Es konnten entweder alle Protokolle gleichzeitig oder nur ein Protokoll aktiviert werden.

LANCOM GS-2300-Serie Änderungen 3.32.0135 SU3

Korrekturen / Anpassungen

→ Der Zufallsgenerator zur Erzeugung von SSH-Schlüsseln generierte nicht genügend unterschiedliche Host-Schlüssel.
Um sicher zu stellen, dass nach der Firmware-Aktualisierung auf LCOS SX 3.32 SU3 genügend unterschiedliche SSH-Host-Schlüssel im Switch zur Verfügung stehen, müssen Sie folgendermaßen vorgehen:

- Öffnen Sie das Webinterface des Switches.
- Wechseln Sie in das Menü ‚Security / SSH'.
- Klicken Sie dort auf die Schaltfläche ‚Regenerate Hostkey'.
- Speichern Sie die Konfiguratiom im Menü ‚Maintenance / Save/Restore' mit der Option ‚Save Start'.
- Starten Sie den Switch mit der Option ‚Maintenance / Restart Device' neu.

Beim Neustart des Switches werden neue SSH-Host-Schlüssel erzeugt.
Siehe auch https://support.lancom-systems.com/knowledge/x/AoCCAg.

LANCOM GS-2300-Serie Änderungen 3.32.0114 RU2

Korrekturen / Anpassungen

→ Bei Switches, welche mit der LANCOM Management Cloud (LMC) verbunden waren, konnte es in seltenen Fällen zu einem SSL-Verbindungsfehler kommen, der dazu führte, dass die Geräte nicht mehr von der LMC verwaltet werden konnten. Lediglich das Monitoring war noch funktional.

→ Wenn der LANCOM Switch einen Netzwerk-Loop erkannt hatte, wurde bisher lediglich die Uhrzeit und der blockierte Port in einer Syslog-Meldung protokolliert. Die Netzwerk-Loop-Erkennung protokolliert nun zusätzlich die Nummer des zweiten beteiligten Ports und gibt zudem eine Information darüber, welcher Port der Sender und welcher Port der Empfänger des Loop Protection Frame war.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0110 RU1

Neue Features

→ Erweiterung der Gerätelogs

→ Erweiterung der PoE-Detection (Legacy Mode)

→ Neuer Schalter für sFlow (Always On)

Korrekturen / Anpassungen

→ Die LANCOM Switches übermittelten MAC-Adressen (z. B. von Supplicants bei 802.1X an einem RADIUS-Server) ausschließlich unter Verwendung von kleinen Buchstaben (z. B. 00-10-a4-23-19-c0). Laut der RFC-3580 müssen jedoch Großbuchstaben verwendet werden (z.B. 00-10-A4-23-19-C0), was nun der Fall ist.

→ Die automatische Umstellung der Uhrzeit auf mitteleuropäische Sommerzeit (MESZ) erfolgte eine Woche zu früh.

→ Aufgrund eines zu geringen internen Daten-Buffers wurden zu große TLV-Pakete (Type-Length-Value) verworfen. In der Folge schlug die Authentifizierung eines Clients via 802.1X an einem RADIUS-Server fehl.

→ Wurde die Weboberfläche des Switches über eine IPv6-Adresse aufgerufen, funktionierte die Anzeige der Online-Hilfe nicht.

→ **Nur GS-2300-Serie:** Wurde einem per LMC verwalteten Switch per Addin-Skript eine feste IP-Adresse zugewiesen, führte dies zu einem unvermittelten Neustart des Switches.

→ **Nur GS-2300-Serie:** Erstellte man eine Skriptspeicherung von einem Switch des Typs **LANCOM GS-2352x**, in welcher bei 26 Ports ein PVID eingetragen ist, so ließ sich diese Skriptspeicherung nicht in das Gerät laden.

→ **Nur GS-2300-Serie:** Wenn auf einem in der LMC verwalteten LANCOM Switch der GS-2300-Serie die LLDP-Funktion für die automatische Geräte-Erkennung verwendet wurde, konnte es zu einem unvermittelten Neustart des Switches kommen.

→ **Nur GS-2300-Serie:** Ein Ping auf die IP-Adresse eines GS-2352(P) wurde vom Switch nicht beantwortet, wenn ein Management-VLAN ungleich 1 verwendet wurde.

→ **Nur GS-2300-Serie:** Bei der Übernahme eines GS-2300 in die LANCOM Management Cloud wurden „Forbidden VLANs“ nicht in die LMC-Konfiguration übernommen.

→ **Nur GS-2300-Serie:** Debug-Informationen zur Analyse eines unvermittelten Neustarts („Watchdog“) konnten per SSH und Telnet nicht vollständig ausgelesen werden.

- → **Nur GS-2300-Serie:** Eine offene SSH-, Telnet- oder Web-Session auf einen über die LMC verwalteten Switch wurde nicht unmittelbar beendet, wenn über die LMC ein neues Haupgerätepasswort auf den Switch ausgerollt wurde.
- → **Nur GS-2300-Serie:** Ein Reboot-Event, welches über SNMP oder die LMC ausgelöst wurde, wurde nicht ins Syslog geschrieben.
- → **Nur GS-2300-Serie:** Das Pairing eines Switch mit der LMC über **LANconfig mittels Aktivierungscode** wurde nicht erfolgreich abgeschlossen. In der Folge befand sich der Switch in einer Endlos-Schleife. Der identische Vorgang über die Weboberfläche oder das Claiming mittels PIN funktionierte hingegen.
- → **Nur GS-2300-Serie:** Der Konfigurationspunkt „Unregistered ICMPv6 Flooding“ unter MLD-Snooping war auf Modellen der GS-2328- und GS-2352-Serien ohne Funktion.
- → **Nur GS-2300-Serie:** Eine fehlerhafte sFlow-Konfiguration führte dazu, dass ein Switch nach einiger Zeit anstatt „Flow Samples“ nur noch „Counter Samples“ gesendet hat und der sFlow Collector keine Daten mehr empfing.
- → **Nur GS-2300-Serie:** Ein GS-2310(P) lieferte bei Abfrage via SNMP für die CU- und SFP-Ports 9 und 10 jeweils die gleiche Port-ID aus. Nun wird für die CU-Ports die Port-ID 9A und 10A, sowie für die SFTP-Ports 9B und 10B ausgeliefert.

LANCOM GS-1300- / GS-2300-Serie Änderungen 3.32.0012 Rel

Neue Features

→ Für SSL- und TLS-Konfigurationen sind nun die anzuwendenden SSL- / TLS-Mindestversionen in einer Drop-Down-Liste auswählbar.

→ Hinweis über noch nicht gespeicherte Konfiguration auf der Konfigurationsoberfläche

→ **Nur GS-2300-Serie:** Scriptingfähigkeit über die LANCOM Management Cloud

Korrekturen / Anpassungen

→ Wenn STP auf den Switch-Ports aktiviert war und diese Konfiguration als „Start-Konfiguration“ gespeichert wurde, konnte es nach einem Kaltstart des Switches vorkommen, dass die Angabe der „Uptime“ im Menü „Configuration > Port Status“ mit 2627 Tagen angegeben wurde.

→ Bei einem Konfigurations-Export in eine *.xml-Datei fehlten die PoE-Konfigurationsparameter für „Power delay“, „Auto checking“ und „Scheduling“.

→ Switch-Ports, bei welchen eine 802.1X Single-/ Multi-Mode Port-Authentifizierung konfiguriert war, wurden nach ca. 4-6 Minuten gesperrt und nach weiteren 4-6 Minuten wieder geöffnet. Der Port- Status wurde immer, auch in den gesperrten Phasen, als „Authorized“ angezeigt.

→ Der Error-String in einer Fehlermeldung wurde auf der Weboberfläche nicht auf die Größe des Meldungsbereichs angepasst.

→ In der Online-Hilfe für die Funktion „Configured link speed“ (im Menü „Port configuration“) fehlten Beschreibungen zu Konfigurationsmöglichkeiten bei unterschiedlichen Switch-Typen.

→ Bei Verwendung der Funktion MAC-based authentication für angeschlossene Access Points, kam es bei einem Wechsel der Switch-Ports (durch WLAN-Roaming) zu einem unvermittelten Neustart, wenn die MAC-Adresse der WLAN-Clients im RADIUS-Server hinterlegt war.

→ Bei Verwendung mehrerer Switches mit aktiviertem RSTP in einer Ringstruktur und gleichzeitig aktivem DHCP-Snooping kam es bei einer hohen Anzahl an Clients (größer 500) zu einer CPU-Last von 100%.

→ Allgemeine Stabilitätsverbesserungen

→ **Nur GS-2300-Serie:** Ein Hauptgerätepasswort, welches über die LANCOM Management Cloud konfiguriert wurde, war in einem Konfigurations-Export als *.xml-Datei nicht vorhanden.

→ **Nur GS-2300-Serie:** Es war keine Online-Hilfe für die Switch-Systeminformationen „LMC pairing state“, „LMC control state“, „Largest free mem block“ und „Free memory“ sowie für die Funktionen „Configuration save“ und „Configuration upload“ vorhanden.

→ **Nur GS-2300-Serie:** Eine automatische Vervollständigung von „show“-Befehlen mit der Tabulator-Taste schlug auf der Kommandozeile aufgrund der Schreibweise des Befehls „show-3rd-party-licenses“ bei allen managed Switches fehl.

→ **Nur GS-2300-Serie:** Bei Switches des Typs GS-2352x konnte es vorkommen, dass auf bestimmten Ports keine ICMPv6-Pakete übertragen wurden.

→ **Nur GS-2300-Serie:** Bei aktivem MLD-Snooping kam es zu Kommunikations-Problemen mit IPv6-Paketen, wenn die Netzwerk-Verbindung zum Client getrennt und anschließend wieder hergestellt wurde. Auch konnte es bei Verwendung von IPv6 zu hohen Paketverlusten kommen.

5. 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.

Support-Hinweise & bekannte Einschränkungen

Aktuelle Support-Hinweise und bekannte Einschränkungen zur aktuellen LCOS SX-Version finden Sie im Download-Bereich unserer Webseite: Allgemeine Support-Hinweise

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