Release Notes

LCOS FX

10.9 RU1

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 Software Release LCOS FX 10.9 Rel.

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. Wird für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Dient zur nachträglichen Weiterentwicklung einer initialen Release-Version und enthält Detailverbesserungen, 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.

3. Unterstützte Hardware

Version 10.9 Rel unterstützt die folgenden Hardware Appliances:

→ LANCOM R&S®Unified Firewalls
UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/760/900/910
→ R&S®UF-50/100/200/300/500/800/900/1000/1200/2000
→ R&S®UF-T10
→ R&S®UTM+100/200/300/500/800/1000/2000/2500/5000
→ R&S®NP+200/500/800/1000/2000/2500/5000
→ R&S®GP-U 50/100/200/300/400/500
→ R&S®GP-E 800/900/1000/1100/1200
→ R&S®GP-S 1600/1700/1800/1900/2000
→ R&S®GP-T 10

Version 10.9 Rel unterstützt die folgenden virtuellen Appliances:

→ LANCOM vFirewall S, M, L, XL
→ R&S®UVF-200/300/500/900

Version 10.9 Rel unterstützt die folgenden Hypervisor:

→ VMware ESX
→ Microsoft Hyper-V
→ Oracle VirtualBox
→ KVM

4. Historie LCOS FX

LCOS FX-Änderungen 10.9 RU1

Korrekturen

→ Es konnte vorkommen, dass die Unified Firewall bei PPPoE- oder DHCP-Verbindungen keine DNS-Auflösung durchführen konnte.

LCOS FX-Änderungen 10.9 Rel

Verbesserungen

→ **Direkte Verlinkung der Administrationsoberfläche zum Handbuch**
Aus den einzelnen Editoren der Weboberfläche wird jetzt direkt auf das passende Handbuch-Kapitel verlinkt.

Hinweis

→ Das Format der exportierten IPsec-Profile ändert sich von zip auf 7zip.

Korrekturen

→ Wenn die AD-Konfiguration in der Benutzerverwaltung aktualisiert wurde, protokollierte die Unified Firewall das Kennwort im Audit-Log.
→ Bei der Verwendung von automatischen Backups wurde die Uhrzeit, zu der ein Backup durchgeführt werden sollte, nicht korrekt gespeichert.
→ LDAP-Benutzer-Accounts, die ein ‚+'-Zeichen im Kennwort besaßen, konnten sich nicht über das Webportal anmelden. Im Frontend wurde die Meldung ausgegeben, dass das Kennwort falsch ist.
→ Lokale Benutzer konnten sich nicht am internen Firewall-Portal anmelden, wenn das Kennwort ein ‚+'-Zeichen enthielt.
→ Wenn in den Namen von IPSec-VPN-Verbindungen Umlaute verwendet wurden, konnten diese Verbindungen nicht exportiert werden.
→ Der NTP-Server einer Unified Firewall konnte über eine VPN-SSL-Verbindung nicht angesprochen werden, da die für den Zugriff erforderlichen Firewall-Regeln nicht erstellt wurden.
→ Für eine IPSec-Verbindung wurden die VPN-Regeln (SAs) mehrfach generiert.
→ Wenn ein DHCP-Server für unterschiedliche Ethernet-Interfaces erstellt und jeweils eine statische IP-Adresse mit dem gleichen Host-Namen hinterlegt wurde, führte dies dazu, dass der DHCP-Server nicht startete. In einem solchen Fall wird jetzt die Meldung „Der Hostname wird bereits beim DHCP-Interface ‚ethx' verwendet." ausgegeben.
→ Wenn bei der Aushandlung einer IKEv2-Verbindung von der Gegenseite ein Traffic-Selector mit Port-Einschränkung empfangen wurde, führte dies zu einem Absturz des VPN-Dienstes (xipsecd).
→ Enthielt der Private Key des in den VPN-SSL-Einstellungen verwendeten Zertifikates das Paragraphen-Symbol (§), wurde der Private Key beim Speichern nicht geschrieben. Dies führte dazu, dass keine VPN-SSL-Verbindung aufgebaut werden konnte.
→ War die Festplatte der inaktiven Unified Firewall in einem HA-Cluster voll, trat nach einiger Zeit ein ‚Hard Disk Watchdog' auf. Dadurch wurde die Unified

Firewall heruntergefahren anstatt diese neu zu starten.

LCOS FX-Änderungen 10.9 RC1

Neue Features

→ **Mit BGP zu einer robusten und effizienten (Standort-) Vernetzung**
Mit dem Einsatz des Routing-Protokolls BGP (Border Gateway Protocol) profitieren Sie nun von noch mehr Effizienz und Stabilität in Ihren Vernetzungs-Szenarien. Durch den gegenseitigen Austausch der besten Pfade aus den Routing-Tabellen der Firewalls ermöglicht BGP, vergleichbar mit einem Navigationssystem, eine schnelle und dynamische Verteilung der Routen, sodass die Pakete optimal auf die Netzwerkpfade verteilt werden können. Auch bei einem Ausfall einzelner Knotenpunkte oder gar ganzer Netzwerkabschnitte finden Ihre Komponenten via BGP einen Weg die Vernetzung aufrechtzuerhalten.

→ **DNS Web Filter — Sicherheit für BYOD ganz ohne Zertifikate**
Auch in Zeiten von hybriden Arbeitsformen mit dem Einsatz von Nutzer-eigenen Endgeräten (Bring your own device, kurz BYOD) können Sie sich auf Ihre Geschäftsintegrität verlassen. So werden DNS-Anfragen, die über den DNS-Server der LANCOM R&S®Unified Firewalls laufen, identifiziert, klassifiziert und gemäß ihrer Kategorien oder der selbst konfigurierten Black- und Whitelists gefiltert. Durch diesen DNS-basierten Schutz blockiert Ihre LANCOM R&S®Unified Firewall unerwünschte und schädliche Seitenaufrufe - sogar auf Geräten, die nicht durch die jeweilige Organisation verwaltet werden. Gerade in BYOD-Szenarien, wie es zum Beispiel in Schulnetzen üblich ist, schützen Sie so Ihr Netzwerk vor Phishing-Angriffen oder dem unbemerkten Herunterladen von schädlicher Software.

Weitere Verbesserungen

→ Der Config-Rollout der LANCOM Managment Cloud auf die LANCOM R&S®Unified Firewalls wurde bedeutend beschleunigt.

→ Bei Supportfällen können Debug-Informationen direkt aus dem Webclient an den Support gesendet werden

Korrekturen

→ Wenn mit LCOS FX 10.7 im Frontend des Reverse Proxy ein lokales Netzwerk als Verbindung hinterlegt wurde, startete nach einem Update auf LCOS FX 10.8 der apache2-Dienst nicht mehr. Dies führte dazu, dass der Reverse Proxy nicht mehr funktionierte.
Wenn eine im Frontend des Reverse Proxy hinterlegte Verbindung keine gültige IP-Adresse bezog, wurde das Frontend mit der IP-Adresse 0.0.0.0 (ANY) erstellt. Dadurch kam es zu Konflikten mit anderen Frontends mit gleicher Portnummer, was ebenfalls darin resultierte, dass der Reverse Proxy nicht funktionierte.

→ Es war möglich, in den DHCP-Server-Einstellungen bei unterschiedlichen Netzwerken BootP-Einträge mit dem gleichen Host-Namen zu hinterlegen. Dies führte dazu, dass die dhcpd-Config ungültig wurde und die DHCP-Adressvergabe nicht mehr funktionierte.

→ Das ‚Interne Portal' war dauerhaft über den Standard-Port 443 erreichbar, auch wenn es deaktiviert wurde.

→ Bei der Konfiguration von N:N NAT für eine VPN-Verbindung wurden die Regeln nur geschrieben, wenn die Netzwerke die gleiche Größe hatten. Bei unterschiedlich großen Netzwerken führte dies dazu, dass die Kommunikation zwischen den Netzwerken nicht möglich war.

→ Der Reverse Proxy funktionierte nicht für die primäre Domain.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de

5. Weitere Informationen

→ Backups der Versionen 9.6, 9.8 und 10.X werden unterstützt.
→ Geräte mit weniger als 4 GB RAM können nicht alle UTM-Features zur gleichen Zeit ausführen.

6. Bekannte Probleme

→ Systemprotokolle und Auditprotokolle werden im High-Availability-Modus nicht synchronisiert.
→ Einige Monitoring-Informationen sind noch nicht verfügbar:
- Anmeldestatus der Benutzer
- Last der Netzwerkschnittstellen

7. 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.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de