Release Notes

LCOS FX
10.12 RU3

Inhaltsübersicht

02 **1. Einleitung**

02 **2. Das Release-Tag in der Software-Bezeichnung**

03 **3. Unterstützte Hardware**

04 **4. Historie LCOS FX**
04 LCOS FX Änderungen 10.12 RU3
05 LCOS FX Änderungen 10.12 RU2
06 LCOS FX Änderungen 10.12 RU1
07 LCOS FX Änderungen 10.12 Rel
08 LCOS FX Änderungen 10.12 RC1

10 **5. Weitere Informationen**

10 **6. Bekannte Probleme**

10 **7. Haftungsausschluss**

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 10.12 RU3.

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 10.12 RU3 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 10.12 RU3 unterstützt die folgenden virtuellen Appliances:

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

Version 10.12 RU3 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

LCOS FX Änderungen 10.12 RU3

Hinweise

Der Einsatz der Firewall-Betriebssystemversionen LCOS FX 10.11 RU3 oder LCOS FX 10.12 RU3 ist auf allen Unified Firewalls mit einer aktivierten Full License erforderlich, damit unsere Kunden auch noch nach dem 30. September 2023 die Antivirus-Funktion wie gewohnt nutzen können. Ohne ein Update auf diese Versionen wird die Antivirus-Funktion der Unified Firewalls ab dem 01. Oktober 2023 jeden Seitenaufruf blockieren, bzw. je nach manuellen Einstellungen sämtlichen Datenverkehr ungefiltert durchleiten.

Nach der Firmware-Aktualisierung auf LCOS FX 10.11 RU3 führt die Unified Firewall keinen automatischen Neustart durch. Die Firmware ist sofort aktiv.
Im Info-Bereich der Firewall-Benutzeroberfläche wird so lange die vorherige Firmware-Version angezeigt, bis eine erneute Anmeldung des Admin-Benutzers erfolgt.
In der LANCOM Management Cloud wird die vorherige Firmware-Version so lange angezeigt, bis ein Neustart der Unified Firewall erfolgt.

Korrekturen

→ Es wurde eine Sicherheitslücke im Border Gateway Protokoll (BGP) behoben (CVE-2023-38802).
→ Die Schlüssel zum Betrieb der Avira Antivirus Engine wurden aktualisiert.
→ Es war möglich, über das Benutzerportal Reflected Cross-Site-Scripting durchzuführen.

LCOS FX Änderungen 10.12 RU2

Korrekturen

→ Nach einem Neustart der Unified Firewall konnte es vorkommen, dass der Dienst für die DHCP-Relay-Schnittstelle nicht funktionierte.

→ In einem Szenario mit zwei WAN-Verbindungen und einer DMZ wurden Anfragen, die über die erste WAN-Verbindung versendet wurden, vom DMZ-Server über die zweite WAN-Verbindung beantwortet.

→ Das Erstellen eines aktuellen Management-Berichts als PDF-Dokument im Menü ‚Management-Bericht / Aktueller Bericht' funktionierte nicht, wenn blockierte Verbindungen protokolliert wurden.

→ Nach einer Änderung der IP-Adressen der ‚primary' und ‚secondary' Firewall in einem HA-Cluster wurden diese nicht in der ‚hosts' Datei aktualisiert. Dies führte dazu, dass die Namen ‚primary' und ‚secondary' nicht mehr aufgelöst werden konnten und dadurch der HA-Cluster nicht mehr aufgebaut werden konnte.
Weiterhin konnte es beim Aufbau des HA-Clusters aufgrund einer Race Condition vorkommen, dass der Application Filter die Kommunikation im HA-Cluster blockierte.

→ Bei Verwendung von Route-based IPSec werden virtuelle Interfaces verwendet. Der dhcprelay daemon unterstützte die virtuellen Interfaces aber nicht, sodass DHCP relay-Pakete nicht über Route-based IPSec-Verbindungen zwischen zwei Standorten übertragen werden konnten.

→ IPSec-Verbindungen mit IKEv2 Redirect zur Weiterleitung an ein anderes Gateway konnten nicht aufgebaut werden, da der IPSec-Dienst (strongswan) sich beendete.

LCOS FX Änderungen 10.12 RU1

Korrekturen

→ Es konnte zu längeren Timeouts zwischen dem Content Filter-Dienst der Unified Firewall und der Bitdefender Cloud kommen. In der Folge kamen Webseiten-Aufrufe nur langsam zustande.

→ Wenn der Content Filter auf DNS-Basis verwendet wurde, konnte es vorkommen, dass Webseiten, die geblockt werden sollten, dennoch angezeigt wurden.

→ Die Intrusion Detection blockierte umgeleitete DNS-Anfragen auf dem Port 10053. In der Folge wurden eingehende Daten von ‚google.com' nicht übertragen.

→ Nach einer Aktualisierung auf LCOS FX 10.11 REL konnte es vorkommen, dass bei aktiviertem DNS-Filter DNS-Anfragen nicht mehr funktionierten.

→ Der ICAP-Server der Unified Firewall erzeugte eine hohe CPU-Auslastung, was zu unregelmäßigen Ausfällen von Internet-Verbindungen führen konnte.

→ Der DNS-Loadbalancer (dnsdist) belegte bei jedem Neu-Laden der DNS-Server-Liste Speicher und gab diesen nicht mehr frei. Dies konnte in einem Szenario mit sehr schlechter Erreichbarkeit der DNS-Server dazu führen, dass sehr viel Speicher reserviert wurde.

→ Ein Neustart des VPN-Dienstes (xipsecd), z. B. bei einem Neustart der Firewall, erzeugte im IP-Tabellen-Regelwerk eine neue virtuelle xfrm-Schnittstelle und sorgte dafür, dass das Regelwerk unnötig größer wurde.

→ In einem Backup-Szenario mit zwei WAN-Verbindungen war der Application Filter auf der Backup-WAN-Verbindung nicht funktionsfähig.

→ Wenn der Content-Filter im DNS-Modus betrieben wurde und DNS-Anfragen ins WAN per Regel erlaubt waren, leitete die Firewall ausgehende DNS-Anfragen auch an sich selbst weiter, wenn kein Content-Filter-Profil ausgewählt war.

LCOS FX Änderungen 10.12 Rel

Korrekturen

→ Bei einem Backup mit einer BGP-Konfiguration, welches unter LCOS FX 10.11 erstellt wurde, konnte die BGP-Konfiguration nach dem Laden in LCOS FX 10.12 RC1 nicht geöffnet werden.

→ Bei einer Abfrage der LLDP-Nachbarn wurden keine Nachbar-Geräte angezeigt, obwohl diese vorhanden waren.

→ Bei einer Anzeige-Vergößerung der WEB-Oberfläche im Browser (z.B. Google Chrome) wurden statt einer Scroll-Leiste zwei Scroll-Leisten angezeigt.

→ In einem Szenario mit mehreren WAN-Verbindungen konnte es vorkommen, dass die Routing-Regeln in eine falsche Routing-Tabelle geschrieben wurden und somit z.B. VPN-Verbindungen nicht zustande kamen, weil diese über die falsche WAN-Verbindung geroutet wurden.

LCOS FX Änderungen 10.12 RC1

Neue Features

→ **Unterstützung für den VPN-Standard ‚WireGuard'**
LANCOM R&S®Unified Firewalls unterstützen ab sofort den VPN-Standard „WireGuard" für eine einfache und schnelle Administration von VPN-Verbindungen. Der Einsatz des Noise-Protokolls sorgt dabei für einen effizienten Handshake, der den Aufbau der VPN-Verbindungen effektiv beschleunigt. Zusätzlich wird durch die Reduktion von Verschlüsselungsparametern ein hoher Datendurchsatz erreicht.

→ **DNS-basierte Firewall-Regeln**
Erstellen Sie ab LCOS FX 10.12 Firewall-Regeln über und zwischen DNS-Objekten für ein einfacheres Management von dynamischen und Software-basierten Netzwerken. Die Verwendung von Host-Namen anstelle von festen IP-Adressen macht die Erstellung von Firewall-Regeln dabei besonders effizient.

→ **Hardware-Monitoring mit grafischer Darstellung**
Die grafische Darstellung aller entscheidenden Systemparameter, wie z.B. CPU, RAM und Festplattenauslastung, bietet einen schnellen und umfassenden Überblick über die Leistung und Auslastung der LANCOM R&S®Unified Firewalls. Die Zuordnung des Ressourcenverbrauchs zu Features und Prozessen ermöglicht es, Engpässe und Schwachstellen schnell zu identifizieren und gezielte Optimierungsmaßnahmen zu ergreifen.

→ **E-Mail-Versand von Security Reportings**
Durch den automatischen Versand des Security Reportings per E-Mail mit einstellbaren Intervallen wird eine effiziente Archivierung und Auditierung ermöglicht. Dies bietet einen klaren Vorteil in Bezug auf die Überwachung und Sicherheit Ihres Netzwerks, da relevante Sicherheitsinformationen zeitnah und zuverlässig zur Verfügung gestellt werden.

Weitere Verbesserungen

→ **BGP-Erweiterungen**

- Unterstützung von Multihop-BGP für die Übertragung von BGP-Paketen durch einen IPSec-Tunnel
- Auswahl der Zieltabelle für gelernte Routen zur Nutzung von Policy-based Routing mit BGP

→ **LLDP Monitoring**

- Unterstützung des Link-Layer Discovery Protocols sowohl als Sender als auch als Empfänger inklusiver der Anzeige der aktuell sichtbaren Nachbarn

→ **Export der Protokolle**

- System-, Alarm- und Auditprotokoll können als PDF, HTML oder CSV exportiert werden

Korrekturen

→ Der DNS-Loadbalancer (dnsdist) belegte bei jedem Neu-Laden der DNS-Server-Liste Speicher und gab diesen nicht mehr frei. Dies konnte in einem Szenario mit sehr schlechter Erreichbarkeit der DNS-Server dazu führen, dass sehr viel Speicher reserviert wurde.

→ Bei einem Verbindungsaufbau einer Client-to-Site IKEv2-Verbindung über eine Internet-Verbindung mit einer Bridge als Verbindungs-Medium wurden die Pakete nicht korrekt durch das Connection Tracking (conntrack) zugeordnet. Dadurch wurden die Pakete verworfen und es war keine Kommunikation zwischen dem VPN-Client und den internen Ressourcen möglich.

→ Der Heartbeat-Test in einer WAN-Verbindung wurde immer als erfolgreich angezeigt, egal welches Argument hinterlegt wurde (sowohl per „ping“ als auch per „tcp_probe“).

→ Nach einem Wechsel der IP-Adresse einer Netzwerk-Verbindung konnte es vorkommen, dass die Änderung nicht in alle Routing-Tabellen übernommen wurde. Dies führte dazu, dass die Kommunikation mit der geänderten Verbindung nicht mehr möglich war.

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

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen. 09/23