Release Notes

LCOS FX
10.11 RU4

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 10.11 RU4
05 LCOS FX-Änderungen 10.11 RU3
06 LCOS FX-Änderungen 10.11 RU2
07 LCOS FX-Änderungen 10.11 RU1
08 LCOS FX-Änderungen 10.11 Rel
10 LCOS FX-Änderungen 10.10 Rel
11 LCOS FX-Änderungen 10.10 RC2
12 LCOS FX-Änderungen 10.10 RC1

13 **5. Weitere Informationen**

13 **6. Bekannte Probleme**

13 **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 10.11 RU4.

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 10.11 RU4 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 10.11 RU4 unterstützt die folgenden virtuellen Appliances:

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

Version 10.11 RU4 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

LCOS FX-Änderungen 10.11 RU4

Korrekturen

→ Es wurde eine Sicherheitslücke im Web-Proxy behoben, durch die Angreifer Daten durch Request/Response-Pakete in HTTPS 1.1 bzw. ICAP durch den Squid-Proxy schmuggeln konnten.

LCOS FX-Änderungen 10.11 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 10.11 RU2

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 eigentlich geblockt werden sollten, trotzdem 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 keine DNS-Anfragen 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.

LCOS FX-Änderungen 10.11 RU1

Korrekturen

→ In einem HA-Cluster-Szenario wurde der Dienst für Content Filtering und Anti-Spam Filtering (bdamserver) nicht automatisch gestartet. Dies führte nach einem Wechsel auf die Slave-Firewall im HA-Cluster dazu, dass Webseiten nicht aufgerufen werden konnten und stattdessen die Blockseite des URL- / Content-Filters angezeigt wurde (Blacklist Unknown).

LCOS FX-Änderungen 10.11 Rel

Migration

Mit LCOS FX-Version 10.11 werden die beiden Services Content-Filter und Anti-Spam von einem neuen, spezialisierten OEM-Partner zur Verfügung gestellt.

Soweit möglich wird die Migration automatisiert durchgeführt. Da die Kategorien zum Teil jedoch nicht immer eindeutig ausgetauscht werden können, sollten Sie Ihre Content-Filter-Konfiguration anschließend überprüfen und Entscheidungen bei unklaren Zuordnungen manuell durchführen.

Abhängig von der Art des Managements und der Anzahl Ihrer LANCOM R&S®Unified Firewalls ergeben sich unterschiedliche Migrationsalternativen:

→ Migration einer einzelnen LANCOM R&S®Unified Firewall
→ Migration von mehreren LANCOM R&S®Unified Firewalls mit Hilfe des hierfür erstellten LANCOM Web-Tools
→ Migration von über die LANCOM Management Cloud verwalteten LANCOM R&S®Unified Firewalls

Wie Sie die Migration zugeschnitten auf Ihre Ausgangssituation ganz bequem durchführen, erfahren Sie in diesem Addendum zu LCOS FX 10.11.

Korrekturen

→ Sicherheitsverbesserungen durch ein Update der OpenSSL-Version auf 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 und CVE-2022-4450)
→ Sicherheitsverbesserungen durch eine Aktualisierung des FRRouting-Protokolls (CVE-2022-37032).
→ Sicherheitsverbesserungen durch eine Aktualisierung von Strongswan auf die Version 5.9.10 (CVE-2023-26463).
→ Aufgrund eines Problems mit der Groß- / Kleinschreibung bei der Angabe des Server-Pfades konnte es vorkommen, dass Reverse Proxy-Verbindungen zu einem Microsoft Exchange-Server nach einer Aktualisierung auf LCOS FX 10.10 REL nicht mehr funktionierten.
→ Es konnte vorkommen, dass der Dienst Suricata im Betrieb abstürzte oder nicht startete. Dies führte dazu, dass Netzwerk-Teilnehmer nicht mehr mit dem Internet kommunizieren konnten, da IDS/IPS die Pakete verwarf.

→ Bei einem Kopier-Vorgang einer IPSec-Verbindung wurde der Kopie die gleiche ID wie der ursprünglichen Verbindung zugewiesen. Dadurch wurde in der Routing-Tabelle 254 nur die ursprüngliche Verbindung angezeigt, nicht aber die Kopie.

→ Während einer DynDNS-Aktualisierung einer durch die LMC verwalteten Unified Firewall konnte es vorkommen, dass die Parameter nicht aktualisiert wurden und stattdessen die alten Parameter in der Konfiguration verblieben.

LCOS FX-Änderungen 10.10 Rel

Verbesserungen

→ Der Reverse Proxy ermöglicht eine direkte Weiterleitung von HTTP auf HTTPS.

→ Die VPN-Gruppen auf dem Desktop erlauben die Angabe einzelner Netzwerke bei IPSec.

Korrekturen

→ In dem zum Traffic Shaping gehörenden Menü ‚Traffic-Gruppen' waren vordefinierte Einträge mit fehlerhaften Werten vorhanden. Es sind jetzt keine vordefinierten ‚Traffic-Gruppen' mehr vorhanden.

→ Wurde bei Verwendung der IDS/IPS eine dort hinterlegte ‚Top Level Domain' (TLD) blockiert (z.B. .biz oder .cloud), blockierte die IPS nachfolgende DNS-Anfragen zu nicht gesperrten TLDs.

→ Die ‚Blockierten Pfade' im Reverse Proxy waren case sensitive, sodass der hinterlegte Pfad nur bei Beachtung von Groß- und Kleinschreibung berücksichtigt wurde.

→ Wenn in einem LMC-Addin ein Parameter fehlerhaft angegeben wurde, funktionierte das Rollback der Konfiguration nicht korrekt.

→ VoIP-Daten, die von Microsoft Teams gesendet wurden, konnten vom Application-Filter der Firewall nicht korrekt erkannt werden.

→ Wenn ein LDAP-Benutzer mit der Schreibweise ‚vorname.nachname' mit der Firewall synchonisiert war, in den Content-Filter-Einstellungen zur Erstellung von Ausnahme-Codes jedoch die Schreibweise ‚Vorname.Nachname' hinterlegt war, konnte der Benutzer keine Ausnahme-Codes erstellen.

→ Bei Verwendung der LCOS FX Version 10.9 RU3 konnte es vorkommen, dass benutzerdefinierte Dienste nach einer unbestimmten Zeit nicht mehr vorhanden waren und stattdesssen lediglich eine UUID angezeigt wurde.

→ Nach einem Neustart der Unified Firewall konnte es vorkommen, dass der DNS-Loadbalancer (dnsdist) einige Zeit keine Verbindung zu den DNS-Servern aufbauen konnte. Dadurch war in diesem Zeitraum keine DNS-Auflösung möglich.

→ Es konnte vorkommen, dass das automatische Wiederherstellen trotz Admin-Login durchgeführt wurde.

→ Wenn die Unified Firewall im HA-Modus betrieben wurde, konnte es nach einer Wiederherstellung zu einem sog. ‚Split Brain' (unerwünschter Zustand eines Computerclusters) kommen.

LCOS FX-Änderungen 10.10 RC2

Neue Features

→ **BGP-Unterstützung für IPSec-Verbindungen**
Durch die Unterstützung von BGP bei aktiven IPSec-Verbindungen profitieren Sie von besserer Lastverteilung und Ausfallsicherheit. Zu diesem Zweck werden Routen nur noch auf aktiven VPN-Tunneln angekündigt.

Weitere Features & Verbesserungen

→ Benachrichtigungs-E-Mails ohne Ereignis lassen sich nun abschalten.

Korrekturen

→ Wenn bei einer durch die LANCOM Management Cloud verwalteten Unified Firewall ein Add-in mit fehlerhaften Parametern ausgerollt wurde, konnte die Konfiguration anschließend korrekterweise nicht ausgerollt werden. Wurde das Add-in anschließend entfernt, kam es beim erneuten Ausrollen weiterhin zu einem Rollout-Fehler.

→ Es konnte vorkommen, dass bei einer IKEv2-Verbindung die Netzbeziehungen (SA) mehrfach erstellt wurden.

→ Bei Verwendung des Application Managements mit Routing des Datenverkehrs von Microsoft Teams über eine bestimmte WAN-Verbindung wurde der VoIP-Datenverkehr nicht korrekt erkannt. Dadurch wurde dieser nicht über die korrekte WAN-Verbindung geleitet.

LCOS FX-Änderungen 10.10 RC1

Neue Features

→ **Add-in-Generator**
Multiplizieren Sie schnell und einfach Ihre ideale Konfiguration von einer Unified Firewall auf beliebig viele von der LANCOM Management Cloud (LMC) gemanagte UFs. Über den neuen Add-In-Generator generieren Sie aus dem Audit-Protokoll einer initial konfigurierten Unified Firewall einfach ganze Add-ins oder auch einzelne Add-in-Abschnitte.

Weitere Features & Verbesserungen

→ **Let‘s Encrypt für den Reverse Proxy**
Bieten Sie nun noch einfacher interne (Web-)Dienste wie z.B. Microsoft Exchange auch öffentlich an. Der Reverse Proxy der Unified Firewalls unterstützt Let‘s Encrypt. So lassen sich mit wenigen einmaligen Handgriffen kostenlose und vertrauenswürdige Zertifikate über die Unified Firewalls einbinden und automatisch verlängern.

→ **Auswahl der Quell-Verbindung bei DNS-Servern**
In Multi-WAN-Szenarien kann jetzt pro Upstream ein z.B. providerspezifischer DNS-Server gewählt werden. Sowohl via PPP als auch DHCP bekannte DNS-Server werden nun stets automatisch über die jeweils passende Leitung angesprochen.

Korrekturen

→ Die Spam-Erkennung per Blacklist funktionierte nicht, wenn im E-Mail-Header das ‚From‘-Feld vom Absender mit UTF-8 codiert wurde.

Hinweis

→ Die Aktualisierung des Benutzerhandbuchs erfolgt mit der kommenden LCOS FX-Version.

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