Release Notes

LCOS FX
11.2 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 11.2 RU1.

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. Unterstützte Hardware

Version 11.2 RU1 unterstützt die folgenden Hardware Appliances:

- → LANCOM R&S®Unified Firewalls
  UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/560/760/900/910/1060
- → 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 11.2 RU1 unterstützt die folgenden virtuellen Appliances:

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

Version 11.2 RU1 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

LCOS FX Änderungen 11.2 RU1

Korrekturen & Anpassungen

→ Wenn in der ‚x-lmc-configd.json' UUIDs für nicht existente Desktop-Verbindungen vorhanden waren, schlug ein Konfigurations-Rollout per LMC fehl.

→ In der LMC-Geräte-Übersicht wurden keine Informationen zur Internet-Verbindung angezeigt, wenn auf der Unified-Firewall eine PPPoE- oder eine Mobilfunk-Verbindung konfiguriert war.

→ Wenn die Let'sEncrypt-Zertifikate für den Reverse-Proxy nicht korrekt erstellt werden konnten, funktionierte dieser nicht. Weiterhin konnten in diesem Fall auch die Reverse-Proxy-Frontends nicht mehr deaktiviert werden.
In einem solchen Fall wird das fehlerhafte Zertifkat jetzt gelöscht und neu erstellt.

→ Eine SAG-Lizenz (Secure Application Gateway) konnte nicht auf einer Unified Firewall mit LCOS FX 11.2 REL aktiviert werden.

→ Es konnten keine Zertifikate ohne das Attribut ‚basicConstraints' in die Unified Firewall importiert werden.

→ Wurde per LMC ein weiterer VPN-Tunnel auf eine Unified Firewall mit vielen konfigurierten VPN-Tunneln ausgerollt, konnte dies zu einer Trennung der VPN-Tunnel führen. Zusätzlich konnte dies dazu führen, dass der Rollout länger als gewohnt dauerte.

→ Durch eine Reihe von Sicherheitslücken im Linux-Tool AppArmor konnten beliebige AppArmor-Profile geladen, ersetzt oder auch gelöscht werden, was Angreifern mit einfachen Berechtigungen durch Local Privilege Escalations die Erlangung von Root-Rechten ermöglichte (CrackArmor).

LCOS FX Änderungen 11.2 Rel

Verbesserungen

→ Support für SAG (SPLA)-Lizenzen

→ Aktualisierte Support-IPs für Web-Client und SSH-Zugriff

Korrekturen & Anpassungen

→ Nach einer Aktualisierung auf LCOS FX 11.2 RC2 konnte es vorkommen, dass eine per LMC verwaltete Unified Firewall die Verbindung zur LMC verlor, da das Zertifikat und der Private Key zur Authentifizierung nicht mehr auf dem Gerät vorhanden waren.

→ Wenn der Applikations-Filter aktiv war und in einer Verbindung verwendet wurde (z.B. LAN zu WAN mit einer Blacklist), lief der Editor zum Erstellen neuer Interfaces (z.B. VLAN- oder Wireguard-Interfaces) in einen Timout und konnte nicht mehr geschlossen werden. Das neu zu erstellende Interface wurde jedoch angelegt.

→ Das Traffic Shaping funktionierte aufgrund von Fehlfunktionen des dafür zuständigen Dienstes nicht ordnungsgemäß.

→ Wenn ein SAML-Benutzer Mitglied mehrerer Desktopgruppen war und sich beim internen Portal der Unified Firewall anmeldete, wurden lediglich die definierten Regeln einer Gruppe angewendet.

→ Es wurde eine Sicherheitslücke behoben, die es angemeldeten Administratoren mit der Berechtigung zur Erstellung von Backups ermöglichte, Code auszuführen.

→ Bei einer Unified Firewall mit LCOS FX 11.2 RC2 im Werkszustand konnte es nach der Konfiguration per LMC vorkommen, dass der zweite Rollout fehlschlug.

→ Beim Konfigurations-Export werden auch die Docker-Container mit exportiert. Wenn Symlinks (Symbolic Link) in den Docker-Containern enthalten waren, führte dies dazu, dass der Export der Docker-Container und somit auch der gesamte Konfigurations-Export fehlschlug.

→ Wenn bei einer durch die LMC verwalteten Unified Firewall mit einer benutzerdefinierten Paketfilter-Regel mit mindestens einem durch die LMC erstellten Desktop-Objekt nach einem fehlgeschlagenen Rollout ein Rollback erfolgte, wurde die benutzerdefinierte Regel gelöscht, konnte durch das Rollback aber nicht wieder hergestellt werden. Dies führte dazu, dass die Kommunikation eingeschränkt war.

LCOS FX Änderungen 11.2 RC2

Verbesserungen

→ Es ist nun möglich, Desktop-Verbindungen zwischen lokalen und LMC-Objekten zu erstellen.

→ Der Reverse Proxy kann Outlook Basic Auth erzwingen.

→ Die LDAP / AD-Anbindung unterstützt jetzt Paging bei der Abfrage der Benutzer und Gruppen, um die Zusammenarbeit mit Active Directory bei mehr als 1.000 Elementen zu verbessern.

→ Die Docker-Anbindung unterstützt jetzt auch die Anmeldung an Azure und Docker Hub, um Docker-Images herunterzuladen.

Korrekturen & Anpassungen

→ Nach einem Konfigurations-Rollout über die LMC wurde die Liste der konfigurierten Syslog-Server gelöscht. Dadurch wurden System-Ereignisse nicht mehr an die Syslog-Server versendet.

→ Regeln für Benutzer-Gruppen, welche sich per SAML authentifizieren, wurden nicht geschrieben. Dies führte dazu, dass für die in der Gruppe enthaltenen Benutzer keine Kommunikation möglich war.

→ VLAN-Interfaces, welche durch die LMC generiert wurden, konnten im Webinterface der Unified Firewall nicht zum Anlegen von Desktop-Objekten verwendet werden, da diese ausgegraut waren.

→ Wenn der Dienst für den HA-Cluster (gpHAd) auf der Master-Firewall keine Antwort vom Dienst für die Lizenz-Verwaltung (gpLicensed) erhielt, sendete diese eine leere Seriennummer an die Slave-Firewall. Die Slave-Firewall entfernte daraufhin die Lizenz, weil die Seriennummer nicht mit der Lizenz übereinstimmte. Bei einem Rollen-Wechsel von Slave auf Master führte dies dazu, dass nicht mehr alle Features vorhanden waren und die Kommunikation somit u. U. nur noch eingeschränkt möglich war.

→ Bei Chromium-basierten Browsern (z.B. Google Chrome oder Microsoft Edge) konnte es vorkommen, dass Desktop-Interaktionen im Webclient verzögert ausgeführt wurden.

→ In einer Routing-Tabelle mit vielen Einträgen wurde im Webclient die ‚Löschen'-Schaltfläche von einem Scroll-Balken überlagert. In der Folge konnte die Schaltfläche nicht verwendet werden.

→ Es konnte vorkommen, dass bei einer externen Kommunikation von einem Microsoft Outlook Client über den Reverse Proxy der Firewall ständig eine Passwortabfrage durchgeführt wurde.

LCOS FX Änderungen 11.2 RC1

Neue Features

→ **Docker-Container-Management*:**

Einführung der Unterstützung für die Verwaltung und Ausführung von Docker-Containern über die REST-API

Key-Features

- Verwaltung von Docker-Containern: erstellen, löschen und aktualisieren von Containern
- Verwaltung von Docker-Netzwerken: erstellen, löschen und aktualisieren von Netzwerken und Anhängen von Containern an diese Netzwerke
- Verwaltung des Lebenszyklus von Containern: starten, stoppen und neustarten von Containern
- Definition von Firewall-Regeln für Docker-Netzwerke
- Persistente Docker-Volumes: Volumes werden durch Firewall-Backups erhalten.
- Abruf von Docker-Images aus Upstream-Registrierungen
- Echtzeitüberwachung: Zugriff auf Containerprotokolle über REST API und Ereignisse über WebSockets

Vorteile

- Verbesserte Sicherheit und Kontrolle über Docker-Container und Netzwerke
- Vereinfachte Verwaltung und Bereitstellung von Containern
- Verbesserte Überwachungs- und Protokollierungsfunktionen
- Nahtlose Integration in bestehende Firewall-Funktionen
- Vereinfachte Handhabung von Containern: Optimierte Verwaltung und Bereitstellung über LMC-Add-ins

API-Dokumentation

- Die interaktive REST-API-Dokumentation ist in der Web-GUI verfügbar.

→ **Lokale Bearbeitung von LMC-Objekten**

- Unterscheidung zwischen zwei Arten von Einstellungen, abhängig vom im LMC konfigurierten Szenario: Einstellungen, die für das vom LMC konfigurierte Szenario unerlässlich sind, und zusätzliche Einstellungen, die nicht unbedingt auf bestimmte Werte festgelegt werden müssen.
- Die zusätzlichen Einstellungen können über die Web-GUI der Firewall entsprechend den Anforderungen des Administrators konfiguriert werden.
- Je nach Szenario können zusätzliche Einstellungen beispielsweise NAT-Einstellungen, IDPS-Ausnahmen, zusätzliche Firewall-Regeln usw. sein.
- Um den Verlust von Einstellungen bei nachfolgenden Konfigurationsrollouts zu vermeiden, führt die Firewall vorhandene zusätzliche Einstellungen mit den Änderungen aus der LMC zusammen.

- Anstatt geänderte Objekte und deren Abhängigkeiten immer neu zu erstellen, versucht die Firewall nun, vorhandene Objekte zu ändern. Dies verbessert die Rollout-Geschwindigkeit und ermöglicht es, mehr Anpassungen des Administrators beizubehalten.
  Änderungen können im Audit-Protokoll überprüft werden.

→ Die von der LMC erstellten Netzwerkschnittstellen können für eigene Desktop-Objekte verwendet werden.
→ Integration von SICCT-Proxy für einen sicheren Betrieb von Kartenlesegeräten im Gesundheitssektor (Telematikinfrastruktur)
→ Aktualisierung und Erweiterung der Bitdefender Content Filter-Kategorien analog LCOS-Betriebssystem
→ Zentrale Syslog-Erfassung in der LANCOM Management Cloud (LMC)
→ SAML: Es gibt die Möglichkeit eine primäre Gruppe auszuwählen. Damit werden nur Gruppen und Benutzer synchronisiert, die innerhalb dieser Gruppe liegen, um die Synchronisation bei großen Organisationen zu beschleunigen.
→ SAML: Es gibt die Möglichkeit den TrustStore zur Verifikation des IDP-Zertifikats zu nutzen
→ SAML: Das Zertifikat/CA des IDP wird per Drop-Down ausgewählt
→ Lets encrypt: Der Typ und die Länge des Schlüssels sind einstellbar: RSA 2048 (legacy), RSA 4096, ECDSA (empfohlen)
→ Der Menüpunkt Proxy CAs wurde in TrustStore umbenannt

Korrekturen & Anpassungen

→ Bei einem neu installierten HA-Cluster konnte es vorkommen, dass die Synchronisation zwischen den Firewalls nicht funktionierte.
→ Die konfigurierte IP-Adresse des SICCT-Proxy (Secure Interoperable Chip Card Terminal) wurde der Netzwerk-Schnittstelle erst nach dem Start des Proxys zugewiesen. Dies führte dazu, dass der SICCT-Proxy diese IP-Adresse nicht verwenden konnte und darüber somit keine Kommunikation möglich war.
→ Wenn eine Konfigurationsänderung durchgeführt wurde, an der ein Host-Objekt mit mehr als 300 Einträgen beteiligt war (z.B. Änderung einer Regel, die dieses Objekt enthielt), fror das Web-Interface ein. Dieser Zustand konnte nur durch einen Neustart der Firewall behoben werden.
→ Wenn in einer Firewall Regel der DMZ-Port hinterlegt war und dieser Eintrag entfernt wurde, sodass kein Port mehr hinterlegt war, konnte im Anschluss das Regelwerk nicht mehr geschrieben werden.

→ Es besteht die Möglichkeit, Unified Firewalls eine LMC-Lizenz zuzuweisen, wenn diese in einem LMC-Projekt mit dem Lizenztyp SPLA (Services Provider Licensing Agreement) betrieben werden. Im Systemprotokoll der Unified Firewall wurde in Abständen von 5 Minuten die Warnmeldung „could not read SPLA license file!“ ausgegeben, wenn das Gerät entweder in einem LMC-Projekt ohne SPLA-Unterstützung oder im Standalone-Betrieb verwendet wurde.

→ Wurde nach der Deaktivierung einer WireGuard-Verbindung die Unified Firewall neugestartet, ignorierte der WireGuard-Dienst (x-wireguardd) die deaktivierte Verbindung und erstellte das zugehörige Interface und die Peer-Konfiguration nicht. Nach der Reaktivierung der WireGuard-Verbindung wurde zwar die Peer-Konfiguration erstellt, aber nicht das WireGuard-Interface. Dadurch war die WireGuard-Verbindung nicht funktionsfähig.

→ Wenn in einem DHCP-Interface im Reiter ‚Herstellerspezifische Optionen‘ eine DHCP-Option ohne Angabe der ‚Hersteller-Kennung‘ angegeben wurde, konnte die Konfiguration zwar nicht erstellt werden, es wurde aber auch keine Warnmeldung angezeigt. Nach einem Logout und anschließendem Login im Webinterface war das DHCP-Interface mit der fehlerhaften DHCP-Konfiguration trotzdem vorhanden. Wurde mehrfach auf ‚Erstellen‘ geklickt, waren anschließend mehrere DHCP-Interfaces für das gleiche Netzwerk vorhanden (für jeden Klick auf ‚Erstellen‘ ein DHCP-Interface). Der DHCP-Dienst war anschließend nicht mehr funktionsfähig.

→ Wurde ein PPP-Interface mit konfiguriertem Traffic Shaping gelöscht, verblieb die Shaping-Konfiguration im Gerät und konnte anschließend nicht gelöscht werden.

→ Bei einem Klick auf das ‚Hilfe‘-Symbol in einer LTA-Gruppe wurde statt des zugehörigen Kapitels aus dem Handbuch die Fehlermeldung „404 Not Found“ ausgegeben.

5. Weitere Informationen

→ Backups der Versionen 9.8 und 10.X werden unterstützt.

→ Geräte mit weniger als 4 GB RAM können nicht alle UTM-Features zur gleichen Zeit ausführen.

6. 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
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de