Release Notes

LCOS FX
10.13 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.

Dieses Dokument beschreibt die Neuerungen der Software Release LCOS FX 10.13 RU7.

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 10.13 RU7 unterstützt die folgenden Hardware Appliances:

- → LANCOM R&S®Unified Firewalls
  UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/760/900/910/1060
- → 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 10.13 RU7 unterstützt die folgenden virtuellen Appliances:

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

Version 10.13 RU7 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

LCOS FX Änderungen 10.13 RU7

Korrekturen

→ Ab LCOS FX 10.13 RU7 sind Protokolle im Suricata-Dienst inaktiv, um den Speicherverbrauch des Dienstes zu verringern.

→ Wenn die Aktivierung einer ansonsten erfolgreich aus der LMC an die Unified Firewall ausgerollten Konfiguration fehlschlug, erfolgte kein Rollback der Konfiguration. Daraus möglicherweise entstehende Inkonsistenzen könnten zu Fehlern bei folgenden Rollouts führen.

→ Es konnte vorkommen, dass eine DHCP-Adresse und die Route nicht entfernt wurden, wenn ein DHCP-Client einen neuen Lease erhielt. In der Folge kam es zu einem IP-Adresskonflikt, da sowohl das alte als auch auch das neue Lease auf dem ETH-Port angeboten wurden.
Zudem konnte es in Szenarien, in denen die Unified Firewall als DHCP-Client konfiguriert war, vorkommen, dass die Firewall bei einem Wechsel der DHCP-Netzwerkadresse auf dem Server keine IP-Adresse per DHCP erhielt. In der Folge konnte es auch zu DNS-Problemen beim Wechsel von einer WAN-Verbindung zu einer anderen WAN-Verbindung kommen.

→ Bei sehr umfangreichen Desktop-Objekten (z.B. Host-Gruppen) stürzte der Regel-Dienst (x-rulesd) bei der Anwendung der Firewall-Regeln ab. In der Folge konnte es u.a. zu Problemen beim Konfigurations-Rollout aus der LMC kommen.

→ Auch wenn das Application-Management oder der HTTP-Proxy deaktiviert war oder werden sollte, wurde die Certification Authority (CA) für die SSL-Inspection validiert. Dies führte dazu, dass das Application-Management bei Verwendung eines abgelaufenen Zertifikat nicht deaktiviert werden konnte.

→ Es konnte bei IPsec mit EAP-TLS Authentifizierung dazu kommen, dass der IPsec-Dienst unerwartet beendet wurde.

→ Es konnte vorkommen, dass VPN-Verbindungen durch einen fehlerhaften Self-Check-Timer von der Unified Firewall unvermittelt getrennt und anschließend erneut aufgebaut wurden.

→ Eine Lizenz, die für eine Unified Firewall UF-1060 eingespielt wurde, zeigte das Gerät als Lizenz für eine UF-960 an.

LCOS FX Änderungen 10.13 RU6

Korrekturen

→ Durch die in LCOS FX 10.13 RU5 eingeführte Fehlerbehebung für die ‚Host Header Forgeries' in Verbindung mit dem transparenten HTTP-Proxy konnte es vorkommen, dass keine Webseite mehr aufgerufen werden konnte.

LCOS FX Änderungen 10.13 RU5

Verbesserungen

→ **Unterstützung für das BGP ‚next-hop-self'-Attribut**
Das ‚next-hop-self'-Attribut wird in der Regel von eBGP-Routern verwendet. Wenn eine Route von eBGP gelernt wird, ersetzt der eBGP-Router das ‚next-hop'-Attribut durch seine eigene Richtung, bevor er die Route an seine iBGP-Peers weiterleitet. Dies ist notwendig, da iBGP-Router nicht in der Lage sind, Router zu erreichen, die nicht Teil ihres eigenen AS sind.

→ **Unterstützung für BFG IP-Präfix-Listen**
IP-Präfixlisten bieten einen leistungsfähigen Mechanismus, um sowohl die Eingabe als auch die Ausgabe von Routing-Informationen zu kontrollieren. So kann für jeden Peer individuell festgelegt werden, welche Routing-Informationen an diesen Peer weitergegeben werden sollen und welche Routing-Informationen von einem Peer gelernt werden sollen.

Hinweis: Beide Einstellungen lassen sich nur über die REST API oder LMC Add-Ins konfigurieren.

Korrekturen

→ Obwohl weitergeleitete Verbindungen, welche von der Unified Firewall blockiert wurden, in der lokalen Statistik der Firewall enthalten waren, wurden diese Meldungen nicht an das Log in der LANCOM Management Cloud (LMC) weitergeleitet.

→ Der Squid-Proxyserver wurde mit aktuellen Sicherheits-Patches versehen.

→ Beim Squid-Proxyserver konnte es im transparenten Modus zu sogenannten ‚Host Header Forgeries' kommen. Diese traten vermehrt bei Verbindungen zu Cloud-Diensten auf und sorgten dafür, dass die Dienste nicht erreicht werden konnten, wenn der transparente HTTPS-Proxy aktiviert war.

→ In einem Szenario, in welchem bei einem Reverse-Proxy ‚Let's encrypt'-Zertifikate verwendet wurden, war der Proxy funktionslos.

LCOS FX Änderungen 10.13 RU4

Neue Features

→ Unterstützung für die Unified Firewall UF-1060
Als performante 2-Höheneinheiten-Appliance (100 GBit/s Firewall- und 12 GBit/s UTM-Durchsatz) rundet die UF-1060 das Portfolio der Unified Firewalls nach oben ab. Mit ihren 8 Erweiterungsslots bietet sie außerdem volle Port-Flexibilität für unterschiedlichste Kundenanforderungen.

Korrekturen

→ Aufgrund eines Fehlverhaltens in der Kommunikation des IPSec-Dienstes konnte es vorkommen, dass bei Routen-basiertem IPSec die Routen nicht angewendet werden konnten, obwohl der IPSec-Tunnel aufgebaut wurde.

→ Beim Rollout mehrerer tausend Block-Regeln über die LMC konnte es zu einem Rollout-Fehler kommen, da das Schreiben der Regeln in die ‚iptables' zu lange dauerte.
Es wurde ein neues Feature implementiert, mit dem Block-Regeln mittels eines Addin-Skripts in die ‚nftables' geschrieben werden können, was deutlich schneller geht. Bei UF-60 und UF-160 können auf diese Weise maximal 5.000 Block-Regeln importiert werden und ab der UF-260 maximal 10.000 Block-Regeln.

LCOS FX Änderungen 10.13 RU3

Hinweis

Das Protokoll für den LMC-WEBconfig-Tunnel wurde neu implementiert. Dies führt zu einer Inkompatibilität zu älteren Versionen des LMC Devicetunnel (service-devicetunnel).
Firewalls, die über die Public LMC verwaltet werden, können direkt aktualisiert werden.
Bei Firewalls, die über Private LMCs verwaltet werden, muss sichergestellt werden, dass die Version der LMC mindestens 1.00.163.0 ist (oder service-devicetunnel Version 16.2.4 oder höher, aufrufbar über ‚Systeminformationen / Service-Informationen / Informationen einblenden'), bevor Firewalls aktualisiert werden.

Korrekturen

→ Es wurde eine Sicherheitslücke im SSH-Protokoll behoben (‚Terrapin'-Sicherheitslücke/CVE-2023-48795).

→ Wenn ein Gruppen-Objekt für Host-Gruppen erstellt wurde, in denen ein Hostname-Eintrag vorhanden war, der ein Teil eines Netzwerks war, welches ebenfalls zur Gruppe gehörte, wurde das Objekt zwar korrekt im Frontend angelegt, es war aber funktionslos, da es im Backend der Unified Firewall ohne Inhalt war.

→ Wenn ein SNAT zu einem Host-Objekt oder eine Host-Gruppe in Richtung WAN hinterlegt war und hinter einer von der Default WAN-IP-Adresse abweichenden WAN-IP-Adresse maskiert werden sollte, so griff das SNAT nicht und es wurde weiterhin hinter der Default WAN-IP-Adresse maskiert.

→ Ein übergeordneter Prozess erzeugte bei einer LANCOM R&S®Unified Firewall UF-60 LTE so viele untergeordnete Prozesse, dass in der Folge keine weiteren Prozesse mehr gestartet werden konnten, da das Maximum erreicht war. Dies führte zu einen unvermittelten Ausschalten oder Neustart der Unified Firewall.

→ Nach einem Update der Unified Firewall auf LCOS FX 10.13 RU1 oder höher waren bei den durch die LMC ausgerollten IPSec-Verbindungen in den zugehörigen Routing-Einträgen die VPN-Interfaces nicht mehr vorhanden. Dies führte dazu, dass über diese VPN-Verbindungen kein Datenverkehr mehr übertragen werden konnte.

→ Bei Verwendung von Host- und Netzwerk-Gruppen wurden für den Appfilter-Dienst (gpAppFilterd) die Einträge in den iptables nicht immer erstellt. Dies führte dazu, dass Daten per Application Routing nicht über die korrekte Verbindung geleitet und Applikationen nicht über den Application Filter blockiert wurden.

→ Wenn in einem Szenario mit einem WAN-Backup ein Wechsel von der Haupt- auf die Backup-Verbindung erfolgte, versuchte die Unified Firewall eine IPSec-Verbindung weiterhin über die Haupt-WAN-Verbindung aufzubauen. Dadurch konnte die IPSec-Verbindung nicht aufgebaut werden, solange die Backup-WAN-Verbindung aktiv war.

LCOS FX Änderungen 10.13 RU2

Korrekturen

→ Bei gleichzeitiger Verwendung einer IPSec-Verbindung und eines Portforwardings wurden über die IPSec-Verbindung gesendete Pakete für die im Portforwarding verwendeten Ports an das Portforwarding-Ziel gesendet statt an das eigentliche Ziel. Dies führte zu einer eingeschränkten Kommunikation über die VPN-Verbindung.

→ Wenn nach einer Aktualisierung auf LCOS FX 10.13 Rel oder 10.13 RU1 in der Konfiguration der Unified Firewall der Mail-Proxy aktiviert war, konnte ein Mailserver (z. B. Microsoft Exchange) keine E-Mails mehr empfangen. Wurde der Inbound-Proxy (SMTP-IN) deaktiviert, funktionierte der E-Mail-Empfang wieder.

→ Nach einer Anmeldung mit Lese-Berechtigung auf der Web-Oberfläche der Unified Firewall wurden Verbindungen zwischen Desktop-Objekten nicht mehr angezeigt.

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

→ Wurde per Web-Interface ein Curl-Befehl mit POST-Daten als Heartbeat eingetragen, setzte die Unified Firewall den Befehl nicht korrekt zusammen. Dies führte dazu, dass der Befehl nicht ausgeführt und stattdessen mit Fehlermeldungen quittiert wurde.

→ Bei Verwendung der UTM-Features ‚Antispam und Contentfilter' konnte es vorkommen, dass der verantwortliche Prozess (bdamserver) einen CPU-Kern zu 100 % auslastete. Dies führte dazu, dass der Aufruf von Webseiten stark verlangsamt war.

→ Beim VPN-Dienst (xipsecd) konnte es vorkommen, dass doppelte Instanzen für eine VPN-Tunnelkonfiguration angezeigt wurden.

LCOS FX Änderungen 10.13 RU1

Hinweis

Bedingt durch eine Anpassung der REST API müssen die LMC Add-Ins ebenfalls entsprechend angepasst werden.

Korrekturen

→ Nach einem Update auf LCOS FX 10.13 REL konnte es vorkommen, dass die Regeln für IPSec-Verbindungen nicht mehr geschrieben werden konnten. Dadurch war die Kommunikation über IPSec-Verbindungen nur eingeschränkt oder gar nicht möglich.

→ Nach dem Einspielen einer LCOS FX 10.13 Rel ISO-Datei und dem Import einer Backup-Datei mit fehlerfreier DNS-Konfiguration funktionierte die DNS-Namensauflösung der Unified Firewall nicht mehr. In der Folge konnten z. B. Anti-Virus-Signaturen nicht mehr aktualisiert werden.

LCOS FX Änderungen 10.13 Rel

Korrekturen

→ Nach der Konfiguration einer IPSec-Verbindung über die LMC konnte es nach einiger Laufzeit vorkommen, dass Monitoring-Informationen nicht immer an die LMC übermittelt wurden. Dies führte dazu, dass die Monitoring-Informationen in der LMC lückenhaft waren.

→ Bei Verwendung des Content Filters im DNS-Webfilter-Modus konnte es vorkommen, dass DNS-Anfragen von Geräten im lokalen Netzwerk blockiert wurden. Dadurch konnten die angefragten Ressourcen nicht von den Geräten aufgerufen werden.

→ In Einzelfällen konnte es vorkommen, dass die Route einer WAN-Verbindung mit Transfer-Netzwerk nicht in die zugehörige Routing-Tabelle geschrieben wurde. In einem solchen Fall war ein Zugriff aus dem Transfer-Netzwerk auf die Unified Firewall nicht möglich, da diese die Antwort an das Default-Gateway im Transfer-Netzwerk sendete statt an das anfragende Gerät.

→ Wenn ein Konfigurations-Menü aufgerufen wurde, dessen Feature nicht in der verwendeten Lizenz enthalten war (z.B. IDS/IPS bei einer Unified Firewall UF-60), wurde das Menü im Lesemodus mit fehlenden Schreibrechten angezeigt.
Bei entsprechenden Konfigurations-Menüs wird jetzt eine Meldung ausgegeben, dass das Feature nicht von der Lizenz unterstützt wird.

→ Bei Apple-Geräten mit iOS 17.0.3 konnte es vorkommen, dass diese keine IPsec-VPN-Verbindung per Standard-iOS-Profil zur Unified Firewall aufbauen konnten, da das Sicherheitsprofil der Unfied Firewall nicht übereinstimmte. In der Firewall-Konfiguration wurde jetzt das Verschlüsselungsprofil ‚AES-GCM 256 bit mit 128 bit ICV' hinzugefügt, sodass die VPN-Verbindungen wieder aufgebaut werden können.

→ Wenn das Webclient-Zertifikat im Menü ‚Firewall / Firewall-Zugriff / Webclient' ausgetauscht wurde, blieb das neue Zertifikat erhalten, bis die Firewall neu gestartet wurde. Nach dem Neustart wurde das Zertifikat wieder auf das Standard-LCOS-FX-Zertifikat zurückgesetzt.

→ Es konnte vorkommen, dass Firmware-Aktualisierungen ausgeführt wurden, obwohl diese laut konfiguriertem Zeitplan zu einem anderen Zeitpunkt installiert werden sollten. Dieses Verhalten trat insbesondere auf, wenn eine Konfiguration von der LMC auf die Unified Firewall ausgerollt wurde.

LCOS FX Änderungen 10.13 RC1

Neue Features

→ **Neuer Dialog zur Verbindung von Desktop-Objekten**
Der neu gestaltete Dialog zur Verbindung von Desktop-Objekten bietet eine optimierte Übersicht für komplexe Firewall-Regeln mit Vererbungen. Die Neuerung umfasst die Anzeige von Regeln in der Tabellendarstellung, die zwischen übergeordneten Objekten definiert sind. Diese erweiterte Darstellung ermöglicht es Ihnen, die gesamte Hierarchie der Regeln auf einen Blick zu erfassen, während sowohl ausgewählte Dienste als auch die Regelungen zwischen übergeordneten Objekten berücksichtigt werden.

Weitere Verbesserungen

→ Für Routen-basierte IPSec-Verbindungen kann die MTU gesetzt werden, um Probleme mit Paketgrößen in einigen Szenarien zu lösen.
→ Zur Überwachung von WAN-Verbindungen kann tcp_probe mit Hostnamen verwendet werden.
→ Zur Überwachung von WAN-Verbindungen kann curl verwendet werden.

Korrekturen

→ Aufgrund einer Umstellung in den Verschlüsselungs-Algorithmen des OpenVPN-Client ab Version 2.6.0 war es nicht möglich, VPN-Verbindungen zur Unified Firewall aufzubauen. Der OpenVPN-Client ab Version 2.6.0 kann jetzt verwendet werden.
→ Ein WEBconfig-Tunnel, der zwischen der LMC und einer Unified Firewall hergestellt wurde, verlor die Verbindung zum Gerät, wenn in der Konfigurationsoberfläche ein Desktop-Objekt angeklickt wurde.
→ Die Leitungsüberwachung einer WAN-Verbindung per ‚tcp_probe' funktionierte nicht korrekt. Dies führte in einem Backup-Szenario dazu, dass die Unified Firewall einen Ausfall der Haupt-Leitung nicht erkannte und nicht auf die Backup-Verbindung wechselte.
→ Nach einer Firmware-Aktualisierung auf LCOS FX 10.12 wurde eine aktivierte Benachrichtigungs-Funktion deaktiviert und musste manuell wieder aktiviert werden.
→ In einem Loadbalancer-Szenario wurden IP-Pakete auch an eine WAN-Verbindung gesendet, wenn diese offline war.
→ Die Verwendung von SNMPv3 mit dem Privacy-Protokoll 3DES war nicht möglich. Die Auswahl für 3DES wurde jetzt aus der Konfiguration entfernt.

→ Es konnten auch Ausnahme-Regeln für IDS/IPS erstellt werden, wenn ein Benutzerprofil ausschließlich ‚Read-Only'-Berechtigungen besaß oder die Lizenz der Unified Firewall abgelaufen war.

→ Bei Verwendung einer Backup-Verbindung konnte es vorkommen, dass Datenverkehr einer IPsec-Verbindung an die Backup-Verbindung gesendet wurde, obwohl diese nicht aufgebaut war.

→ Für die ‚Multi-WAN-Gewichtung' konnten Werte zwischen 1 und 256 vergeben werden, obwohl der Kernel nur einen Maximalwert von 253 erlaubt. Wurde ein Wert zwischen 254 und 256 hinterlegt, funktionierte die Internet-Verbindung nicht.
Es können jetzt nur noch Werte zwischen 1 und 253 vergeben werden.

→ Ein Re-Keying mit dem Hash-Algorithmus SHA1 führte bei einer IPSec-Verbindung zu einem Verbindungsabbruch und anschließendem Neuaufbau Weiterhin wählte die Unfified Firewall bei einer IPsec-Verbindung mit mehreren Hash-Algorithmen den schlechteren Algorithmus aus (z.B. SHA-256 bei Verwendung von SHA-256 und SHA-512).

→ In Einzelfällen konnte es vorkommen, dass der Dienst ‚suricata' sehr viele Fehlermeldungen generierte und auf der Festplatte speicherte, bis diese voll war.

Weitere Informationen

→ SHA1, MD5 und 3DES wurden aus allen IPSec-Standardprofilen entfernt. Falls Sie IPSec-Verbindungen mit veralteten Gegenstellen verwenden, können SHA1, MD5 und 3DES mit benutzerdefinierten Profilen weiterhin verwendet werden. Aus Sicherheitsgründen wird von der Verwendung von SHA1, MD5 und 3DES dringend abgeraten!

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. 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