Release Notes

LCOS FX
10.13 RU2

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 RU2.

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 RU2 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 10.13 RU2 unterstützt die folgenden virtuellen Appliances:

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

Version 10.13 RU2 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

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