Release Notes

LCOS FX 10.11 RU4

Table of contents

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within software release LCOS FX 10.11 RU4.

2. The release tag in the software name

Release Candidate (RC)
A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release-Version (REL)
The release has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions. Recommended for use in productive environments.

Release Update (RU)
This is a further development of an initial release version and contains minor improvements, bug fixes and smaller features.

Security Update (SU)
Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis.

3. Supported hardware

Version 10.11 RU4 supports the following 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 supports the following virtual appliances:

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

Version 10.11 RU4 supports the following hypervisors:

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

4. History LCOS FX

LCOS FX improvements 10.11 RU4

Bugfixes

→ Fixed a vulnerability in the web proxy that allowed attackers to smuggle data through the Squid proxy using request/response packets in HTTPS 1.1 or ICAP.

LCOS FX improvements 10.11 RU3

Notes

The use of the firewall operating system versions LCOS FX 10.11 RU3 or LCOS FX 10.12 RU3 is required on all Unified Firewalls with an activated Full License so that our customers can still use the antivirus function as usual after September 30, 2023. Without an update to these versions, the antivirus function of the Unified Firewalls will block every page call from October 01, 2023, or, depending on manual settings, pass through all data traffic unfiltered.

After the firmware upgrade to LCOS FX 10.11 RU3, the Unified Firewall does not perform an automatic reboot. The firmware is active immediately.
In the info area of the firewall user interface the previous firmware version is displayed until the admin user logs in again.
In the LANCOM Management Cloud, the previous firmware version is displayed until the Unified Firewall is restarted.

Bugfixes

→ A vulnerability in the Border Gateway Protocol (BGP) has been fixed (CVE-2023-38802).
→ The keys for Avira Antivirus Engine operation have been updated.
→ It was possible to perform cross-site scripting via the Reflected user portal.

LCOS FX improvements 10.11 RU2

Bugfixes

→ Longer timeouts could occur between the content filtering service of the Unified Firewall and the Bitdefender cloud. As a result, web page calls were slow.

→ When the content filter was used on a DNS basis, it could happen that websites that were supposed to be blocked were displayed anyway.

→ Intrusion detection blocked redirected DNS requests on port 10053. As a result, incoming data from ‘google.com’ was not transmitted.

→ After an update to LCOS FX 10.11 REL it could happen that DNS queries no longer worked when the DNS filter was activated.

→ The Unified Firewall’s ICAP server generated a high CPU load, which could lead to irregular Internet connection failures.

→ The DNS load balancer (dnsdist) occupied memory every time the DNS server list was reloaded and did not release it. This could lead to a lot of memory being reserved in a scenario with very poor accessibility of the DNS servers.

→ A restart of the VPN service (xipsecd). e.g. when the firewall was restarted, created a new virtual xfrm interface in the IP table rule set and caused the rule set to grow unnecessarily.

LCOS FX improvements 10.11 RU1

Bugfixes

→ In an HA cluster scenario, the content filtering and anti-spam filtering service (bdamserver) was not started automatically. After switching to the slave firewall in the HA cluster, this resulted in web pages not being accessed and the URL / content filter block page being displayed instead (Blacklist unknown).

LCOS FX improvements 10.11 RelI

Migration

With LCOS FX version 10.11, content filtering and anti-spam services are provided by a new, specialized OEM partner.

As far as possible, the migration will be automated. However, in some cases the categories cannot always be exchanged exactly, so you should check your Content-Filter configuration afterwards and make decisions manually if the assignments are unclear.

Depending on the type of management and the number of your LANCOM R&S®Unified Firewalls, there are different migration alternatives:

→ Migration of a single LANCOM R&S®Unified Firewall
→ Migration of multiple LANCOM R&S®Unified Firewalls using the LANCOM web tool created for this purpose.
→ Migration of LANCOM R&S®Unified Firewalls managed via the LANCOM Management Cloud

This addendum to LCOS FX 10.11 explains how you can conveniently migrate your LANCOM R&S®Unified Firewalls in a way that is tailored to your situation.

Bugfixes

→ Security improvements due to an update of the OpenSSL version to 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 and CVE-2022-4450)
→ Security improvements due to an update of the FRRouting protocol (CVE-2022-37032)
→ Security improvements due to an update of Strongswan to version 5.9.10 (CVE-2023-26463)
→ Due to a case sensitivity issue when specifying the server path, it could happen that reverse proxy connections to a Microsoft Exchange server no longer worked after upgrading to LCOS FX 10.10 REL.
→ It could happen that the Suricata service crashed or did not start during operation. This resulted in network subscribers no longer being able to communicate with the Internet because IDS/IPS dropped the packets.

→ During a copy operation of an IPSec connection, the copy was assigned the same ID as the original connection. As a result, only the original connection was displayed in the routing table 254, but not the copy.

→ During a DynDNS update of a Unified Firewall managed by the LMC it could happen that the parameters were not updated and instead the old parameters remained in the configuration.

LCOS FX improvements 10.10 Rel

Improvements

→ The reverse proxy enables direct forwarding from HTTP to HTTPS.

→ The VPN groups on the desktop allow you to specify individual networks with IPSec.

Bugfixes

→ In the ‘Traffic Groups’ menu belonging to Traffic Shaping, there were predefined entries with incorrect values. There are now no more predefined ‘Traffic Groups’.

→ When IDS/IPS was used, if a ‘Top Level Domain’ (TLD) stored there was blocked (e.g. .biz or .cloud), the IPS blocked subsequent DNS queries to TLDs that were not blocked.

→ The ‘Blocked paths’ in the reverse proxy were case sensitive, so the stored path was only considered if it was case sensitive.

→ If a parameter was specified incorrectly in an LMC addin, the rollback of the configuration did not work correctly.

→ VoIP data sent from Microsoft Teams could not be correctly detected by the firewall’s application filter.

→ If an LDAP user with the spelling ‘firstname.lastname’ was synchronized with the firewall, but the spelling ‘Firstname.Lastname’ was stored in the content filter settings for creating exception codes, the user could not create exception codes.

→ When using LCOS FX version 10.9 RU3 it could happen that user-defined services were no longer available after an unspecified time and instead only a UUID was displayed.

→ After a restart of the Unified Firewall it could happen that the DNS load balancer (dnsdist) could not establish a connection to the DNS servers for some time. As a result, DNS resolution was not possible during this period.

→ It could happen that the automatic restore was performed despite admin login.

→ If the Unified Firewall was operated in HA mode, a so-called ‘split brain’ (undesirable state of a computer cluster) could occur after a recovery.

LCOS FX improvements 10.10 RC2

New features

→ **BGP support for IPSec connections**
By supporting BGP on active IPSec connections, you benefit from better load balancing and resilience. For this purpose, routes are announced only on active VPN tunnels.

More features & improvements

→ Notification emails without event can now be turned off.

Bugfixes

→ If an add-in with incorrect parameters was rolled out on a Unified Firewall managed by the LANCOM Management Cloud, the configuration could not be rolled out afterwards, which was correct. If the add-in was subsequently removed, a rollout error still occurred when rolling out again.
→ It could happen that the network relationships (SA) were created multiple times for an IKEv2 connection.
→ When using Application Management with routing of Microsoft Teams traffic over a specific WAN connection, VoIP traffic was not detected correctly. As a result, it was not routed over the correct WAN connection.

LCOS FX improvements 10.10 RC1

New features

→ **Add-in Generator**

Quickly and easily multiply your ideal configuration from one Unified Firewall to any number of UFs managed by the LANCOM Management Cloud (LMC). Using the new Add-in Generator, you can easily generate entire add-ins or even individual add-in sections from the audit log of an initially configured Unified Firewall.

More features & improvements

→ **Let's Encrypt for the reverse proxy**

Now it is even easier to enable public access to internal (web) services such as Microsoft Exchange. The reverse proxy of the Unified Firewalls supports Let's Encrypt. This means that free and trusted certificates can be integrated and automatically be renewed via the Unified Firewalls in just a few simple steps.

→ **Selection of the source connection for DNS servers**

It is now possible to select, for example, a provider-specific DNS server per upstream in multi-WAN scenarios. DNS servers known via PPP as well as DHCP are now always automatically addressed via the appropriate line.

Bugfixes

→ Spam detection via blacklist did not work if the 'From' field in the e-mail header was encoded with UTF-8 by the sender.

Note

→ The user manual will be updated with the upcoming LCOS FX version.

5. Further information

→ Backups of versions 9.6, 9.8 und 10.X are supported.
→ Devices with less than 4 GB of RAM can not execute all UTM features simultaneously.

6. Known issues

→ System- and audit protocols are not synced when operating in high availability mode.
→ Some monitoring information is not yet available:
- User login status
- Network interfaces load

7. Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com