RELEASE NOTES

LCOS SX
5.30 SU3

Table of contents

02 **1. Preface**

03 **2. The release tag in the software name**

03 **3. Note on the firmware update**

04 **4. New features, improvements, and history**
04 LCOS SX 5.30.0365 SU3
05 LCOS SX 5.30.0363 RU2
06 LCOS SX 5.30.0311 RU1

07 **5. Common advice**
07 Disclaimer
07 Support notes & known issues

ROHDE&SCHWARZ
Make ideas real

1. Preface

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

LCOS SX 5.3x is the operating system for the R&S®LANCOM switches CS-8132F and YS-7154CF.

The following LCOS SX operating systems are also available for other R&S®LANCOM switches:

LCOS SX 5.2x is the operating system for all R&S®LANCOM switches of the XS-5100, XS-4500, and GS-4500 series, as well as for the R&S®LANCOM XS-6128QF.

LCOS SX 4.30 is the operating system for all R&S®LANCOM switches of the series XS- / GS- / IGS-3000, and GS-2400.

LCOS SX 3.34 is the operating system for all R&S®LANCOM switches of the GS-2300 and GS-1300 series.

The release notes for these device series can be found as usual on the Rohde & Schwarz Networks and Cybersecurity website in the download area of the respective switch.

This document describes the new features of the LCOS SX software release 5.30 SU3 as well as the changes and improvements to the previous version.

Devices delivered with LCOS SX 5.00 or higher automatically connect to the R&S®LANCOM Management Cloud (R&S®LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the R&S®LMC, this feature can be disabled at any time on the device's WEBconfig under "Configuration > LMC". You can manually re-enable the usage of the R&S®LMC whenever you want.

2. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by Rohde & Schwarz Networks and Cybersecurity and includes new operating system featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)

The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)

A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)

Contains important security fixes for the respective operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Note on the firmware update

Never disconnect the switch from the power supply during a firmware update, as the device will not start properly if the update process is aborted.

Please make sure to **back up your configuration files** before updating your R&S®LANCOM devices to a new firmware version!
Due to the partly extensive feature enhancements, a **downgrade** to the old firmware is **no longer possible** automatically **without such a backup**.
Please note that different firmware files may be available for your device.

4. New features, improvements, and history

LCOS SX 5.30.0365 SU3

Bug fixes

- A security vulnerability in the Linux TCP/IP stack, described in CVE-2026-98432, has been fixed.

LCOS SX 5.30.0363 RU2

Bug fixes

- When two VPC nodes (VPC Node 1 and VPC Node 2) switched roles, the rule that allowed orphan ports to communicate via the VPC peer link was deleted on the new primary node (VPC Node 2). As a result, communication via the orphan ports was no longer possible.
- After a VPC node is started, it is in the 'READY' state. When both VPC nodes are in the 'READY' state and have detected each other, they simultaneously perform the 'election process' to determine which node will be primary and which will be secondary. In a spanning tree scenario, after a role change, the link aggregation group of the downlink port on the new primary node could sporadically remain in the 'Unknown' state instead of switching to 'Forwarding'. This resulted in communication via the downlink port no longer being possible.
- The LANCOM CS-8132F does not support stacking, which is why the console command "show switch" is not available. When reading the Technical Support Log, this caused the process to abort after the "show switch" command, resulting in an incomplete Technical Support Log.
- When rolling out a switch configuration via the LMC, the IP interfaces are first deleted and then recreated. During this process, it could happen that individual IP interfaces were not created, meaning that communication was not possible on these interfaces.
- When a configuration rollout was performed in a scenario managed by LMC with VPC configuration, all link aggregation groups on the VPC nodes were first deleted and then recreated. This resulted in complete packet loss on the link aggregation groups until they were available again.
- In rare cases, the LMC client might send new configuration parameters to the LMC if the SNMP interface of the switch restarted or crashed. This resulted in the LMC client sending empty strings to the LMC, which the LMC interpreted as '-57'. The rollout via the LMC was then no longer possible.
- If the switch received a DHCP offer with a gateway that was located in a different subnet than the assigned IP address, the switch did not log this. In this case, the warning message "Address x.x.x.x update failed due to incorrect parameters in IP/Subnet/Gateway" is now displayed.
- Under certain conditions, the active port speed configuration does not correspond to the configured selection. This meant that auto-negotiation could be active despite deviating settings. In future, invalid configurations will be rejected by the device and must be adjusted manually on both link partners to ensure consistency.

LCOS SX 5.30.0311 RU1

New features

- Functionality extended to include SFP autosensing of plugged-in transceivers and thus automatic configuration of the optical connection link

  Note: The new default for this function is 'Enabled'. Please ensure that the port speed configuration matches the cable, especially when using Direct Attach Cables (DAC) before updating.
- Functionality extended to include orphan ports in the VPC protocol, enabling connection of clients without LAG support (e.g., hypervisor)
- Support for TLS 1.3
- The permitted password length for SNMP users has been increased from 32 to 128 characters.

Bug fixes

- When using a private VLAN, the management VLAN (VLAN 1 in the default configuration) could not be added to the permitted VLANs. As a result, it was no longer possible to access the switch configuration on the ports with the private VLAN.
- If the 'Management Address' in the 'Switching / LLDP / Remote Devices' menu remained empty, the string "nil" was displayed instead of an empty field.
- Adjustments to the 'DNS source interface' parameter were not saved as boot-persistent. This meant that after saving the configuration as the startup configuration and then restarting the switch, the parameter was reset to its default value.
- When obtaining time via NTP, the message "no time source" was displayed in the web interface in the 'System / Advanced Configuration / Time Zone / Summary' menu under 'Time Source'.

5. Common advice

Disclaimer

Rohde & Schwarz Networks and Cybersecurity does not take any guarantee and liability for software not developed, manufactured or distributed by Rohde & Schwarz Networks and Cybersecurity, especially not for shareware and other extraneous software.

Support notes & known issues

Latest support notes and known issues regarding the current LCOS SX version can be found in the download area of our website: Common support tips

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

ROHDE&SCHWARZ
Make ideas real