CryptoServer LAN OS

Release Notes

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com

Document Version	5.4.0
Product Version	5.4.0
Date	2025-05-09
Document No.	2024-0023
Status	**PUBLISHED**

Table of Contents

1 Introduction

Cryptoserver LAN 5.4.0 introduces various enhancements and fixes issues found in previous releases. Please consult the following sections for details.

Please review this document to be informed of any new features and changes introduced by this new release and especially any pre-conditions to notice.

2 List of enhancements

This release of CSLAN OS 32 bit focuses on significant security enhancements, including a large number of CVE (Common Vulnerabilities and Exposures) bug fixes, an update to the latest stable version of OpenSSH, and an update to the *csxlan* network daemon component to address a buffer overrun vulnerability. These updates improve the overall stability and security of the system.

2.1 CVE fixes

This release incorporates patches for a large number of CVEs in various components, including:

- CVE-2023-48795
- CVE-2017-5932
- CVE-2019-18276
- CVE-2022-2068
- CVE-2022-1292
- CVE-2021-3711
- CVE-2019-9924
- CVE-2018-15473

2.2 OpenSSL and OpenSSH Update

LANOS has been updated with Openssl 3.2.0 and OpenSSH 9.6p1

2.3 CSXLAN component update

A critical update to the csxlan component resolves a buffer overrun vulnerability

3 List of bug fixes

The following issues have been resolved in Cryptoserver LAN OS 5.4.0

Reference	Component	Issue
EGL-661 EGL-402 EGL-401 EGL-400 EGL-34	OpenSSL	updated openssl 3.2.0 Fix CVE-2022-2068 Fix CVE-2022-1292 Fix CVE-2021-3711 Fix CVE-2018-15473
EGL-601	OpenSSH	SSH updated to fix CVE-2023-48795
EGL-452	csxlan	The csxlan daemon now checks the maximum length of a packet (0x40000) and returns E_CSA_LX_WRITE_703 (request rejected by CS2) when the packet is too long.
EGL-404 EGL-403 EGL-397	bash	Updated bash 5.2 Fix CVE-2017-5932 Fix CVE-2019-18276 Fix CVE-2019-9924
EGL-28	cslan	Fixed typo in set_sshd_config.sh help text

4 List of known issues

There aren't any known issues with CryptoServer LAN OS 5.4.0.

5 Hardware details

The table below lists the compatible hardware platform for this release

HSM model	***Hardware platform***
CryptoServer Se12/52/500/1500 PCIe	CryptoServer Se-Series Gen2 PCIe card, hardware version >= 5.1.0.0, Bootloader >= 5.00.0.0
CryptoServer CSe10/CSe100 PCIe	CryptoServer CSe-Series PCIe card, hardware version >= 4.0.2.0, Bootloader >= 4.0.0.0

6 Legal Notices

7 Older Releases - 5.3.0

7.1 List of enhancements - 5.3.0

The following enhancements have been added in Cryptoserver LAN 5.3.0

- Support for terminal types xterm-color, xterm-color256 and screen was added.
- Name resolution tools nslookup, host and dig were added to the CSLAN OS.
- Additional firewall rules were added to support DNS queries larger than 512 octets. For this reason, TCP port 53 for IPv4 and IPv6 is now allowed.
- Support leap second smearing with Network Time Protocol NTP. To configure leap smearing, the file /etc/ntp.conf must contain the following line: leapsmearinterval 86400
- More stringent access control and security settings for mitigation of potential security risks:
    - Enable authorization for Linux single user mode to mitigate risks in case an attacker gets physical access to the HSM appliance.
    - Disable ICMP redirect support.
    - Restrict User's home directory mode.
    - Enable logging of LOG_AUTHPRIV messages in case any application from a customer package generates such LOG_AUTHPRIV messages.
- Configuration of TCP port along the IP address (referred as CS2Address) in the NTPClient section of /etc/csxlan.conf , to support changing the csxlan network port itself from 288 to some other TCP port.
- Update of NTP to version 4.2.8p15, addressing vulnerabilities of previous versions 4.2.8
- Description of how ‘transactions per minute’ is computed by CSLAN in the CryptoServer LAN Manual for System Administrators.

7.2 List of bug fixes - 5.3.0

The following issues have been resolved in Cryptoserver LAN 5.3.0

Reference	Component	Issue
HSM-13249	NTP	ntpclient can't be used anymore when you change the csxlan TCP port
HSM-10467	Display admin	CryptoServer LAN reports 0xffff as load
EGL-147	CSLAN	Audit message “[NOTICE] Starting display daemon. CSLan version 5.2.0” shows wrong version number
EGL-17	Display admin	Function LoadFWDecKey from the display panel doesn't work anymore.

7.3 List of known issues - 5.3.0

There aren't any known issues with CryptoServer LAN 5.3.0.