ALEOS 4.9.7

RELEASE NOTES

ALEOS 4.9.7 Release Notes

ALEOS 4.9.7 is for AirLink GX450 and ES450 gateways. These gateways are no longer for sale, as per their end-of-sale announcements available on The Source. ALEOS software maintenance will continue for these gateways in accordance with their end-of-sale details.

Sierra Wireless encourages all customers to maintain their AirLink routers with the current ALEOS release and security patches via our AirLink Management Service (ALMS). Sierra Wireless tests and validates upgrades from the previous two major software releases. If you have routers running an ALEOS release older than the previous two major releases it is recommended that you follow the tested and supported upgrade path.

In addition, other than basic questions that can typically be answered in our existing product documentation, Sierra will only provide technical support for the current and the previous two major software releases via our technical support organization. For example, the current version of ALEOS is 4.9.7 and we continue to support ALEOS 4.9.6 and ALEOS 4.9.5. If you have a support issue with a version prior to ALEOS 4.9.5, you will be asked to upgrade to a supported version before engaging our technical support organization. Our testing of downgrades involves first installing the downgraded version, and then performing a factory reset. We do not provide technical support on routers that were not factory reset after a downgrade was performed. See the table below.

ALEOS Release	Support Level	Upgrade Path
ALEOS 4.9.7	Supported	n/a
ALEOS 4.9.6	Supported	Upgrade directly to 4.9.7
ALEOS 4.9.5	Supported	Upgrade directly to 4.9.7
Previous ALEOS Releases	Limited support. Upgrade to supported release for technical support	1. First upgrade to ALEOS 4.5.1. 2. Then upgrade to ALEOS 4.9.6. 3. Then upgrade to ALEOS 4.9.7.

Sierra Wireless recognizes that our customers deploy devices in a wide range of network environments with varying configurations. It is always good practice to install a new ALEOS release with the planned operation workflow on a few trial devices to ensure that standard operation is maintained within your environment before deploying the new release across your fleet of AirLink devices. For more information, please see the application note Testing AirLink Devices Before Deployment.

Note: Devices manufactured on ALEOS 4.9.6 or later or devices that are reset to factory default on ALEOS 4.9.6 or later have the ACEmanager local access restricted to HTTPS only. ACEmanager should then be accessed using the default 9443 port: https://192.168.13.31:9443/

Note: ALEOS 4.9.7 supports TLS 1.3, TLS 1.2, and removes support for TLS 1.0. and 1.1.

Important Notice

Applicable to ALEOS 4.9.0 and later releases.

As part of Sierra Wireless's continued commitment to ensuring the highest level of security on all AirLink devices, the upgrade process for this release will detect the following potentially insecure device configurations and make corresponding configuration changes to mitigate the potential security impact:

- If User has a default password—Access to Telnet/SSH and server-initiated MSCI over the cellular interface will be disabled. Users of these services are advised to set a strong, unique User password prior to upgrading.
- If Sconsole has a default password—The account will be disabled until a password is set. Users of reverse telnet are advised to set a strong, unique Sconsole password before upgrading.
- If DMZ is set to automatic and the device is not using Public IP (DMZ Enabled is set to Automatic and Host Connection Mode is not set to Ethernet Uses Public IP)—DMZ will be disabled. Users of DMZ but not Public IP are advised to set DMZ Enabled to Manual before upgrading.

If a device has already been upgraded these services can be re-enabled using ACEmanager or AirLink Management Service (ALMS).

In addition to the above changes, the viewer account has been removed and will no longer be accessible in this release.

New Features

SMS	
	Added the following settings to the Preserve Core Settings (Reset to Factory Default mode) list: • SMS Mode • SMS Prefix • SMS Password • Enabled Trusted Phone • Trusted Phone List The SMS Password is now reset after resetting the gateway to factory defaults in "Reset All" mode.
	Added an SMS command to change the Reset to Factory Default "Reset Mode" of the gateway.
	Added an SMS command to perform a Reset to Factory Default.
Telnet/SSH	
	Modified the Telnet/SSH timeout so that it is no longer affected by system time changes.

Security Enhancements

General
Updated openvpn to version 2.5.6.
Removed https support to weak ciphersuites in the TLS configuration.
SSH server: Updated dropbear to version 2020.81 and disabled weak ciphers.
Updated openssl 1.0 to openSSL 1.1 (version 1.1.1n).
Security and CVE Vulnerabilities
Addressed potential vulnerabilities related to CVE-2019-17133.
Addressed potential vulnerabilities related to CVE-2016-3134.
Addressed potential vulnerabilities related to CVE-2017-7895.
Addressed potential vulnerabilities related to CVE-2016-9555.
Addressed potential vulnerabilities related to CVE-2015-1421.
Addressed potential vulnerabilities related to CVE-2022-28391.
Updated OpenVPN to address potential vulnerabilities related to CVE-2022-0547.
Addressed potential vulnerabilities related to CVE-2014-5461.
Removed ncurses from ALEOS, updated procps, and removed openl2tp to address potential vulnerabilities related to: CVE-2022-29458, CVE-2019-17594, CVE-2019-17595, CVE-2019-15548, CVE-2019-15547, CVE-2021-39537, and CVE-2018-1121.
Updated zlib to address potential vulnerabilities related to: CVE-2018-25032, CVE-2016-9843, CVE-2016-9841, CVE-2016-9842, and CVE-2016-9840.
Updated libtar to address potential vulnerabilities related to CVE-2013-4397 and CVE-2013-4420.
Updated tcpdump to address potential vulnerabilities related to CVE-2020-8037 and CVE-2018-16301.
Updated syslog-ng to address potential vulnerabilities related to CVE-2020-8019.
Updated openvpn to address potential vulnerabilities related to CVE-2020-15078.
Updated openSSL to address potential vulnerabilities related to: • CVE-2016-7798 • CVE-2018-5407 • CVE-2018-0734 • CVE-2018-16395 • CVE-2019-1547 • CVE-2019-1551 • CVE-2019-1552 • CVE-2019-1559 • CVE-2019-1563 • CVE-2020-1968 • CVE-2020-1971 • CVE-2021-3712 • CVE-2021-4160 • CVE-2021-23840 • CVE-2021-23841 • CVE-2022-0778

Updated openldap to address potential vulnerabilities related to:

- CVE-2022-29155
- CVE-2020-36221
- CVE-2020-36222
- CVE-2020-36223
- CVE-2020-36224
- CVE-2020-36225
- CVE-2020-36226
- CVE-2020-36227
- CVE-2020-36228
- CVE-2020-36229
- CVE-2020-36230
- CVE-2021-27212
- CVE-2015-3276

Addressed potential vulnerabilities related to CVE-2019-17362.

Updated libpcap to address potential vulnerabilities related to:

- CVE-2019-15163
- CVE-2019-15164
- CVE-2019-15165
- CVE-2019-15161
- CVE-2019-15162

Addressed potential vulnerabilities related to CVE-2021-43618.

Updated glib to address potential vulnerabilities related to CVE-2020-35457, CVE-2021-27218, and CVE-2021-27219.

Updated flex to address potential vulnerabilities related to CVE-2016-6354 and CVE-2015-1773.

Updated curl to address potential vulnerabilities related to:

- CVE-2022-22623
- CVE-2021-22926
- CVE-2021-22946
- CVE-2021-22897
- CVE-2021-22922
- CVE-2021-22923
- CVE-2021-22925
- CVE-2021-22947
- CVE-2021-22898

Addressed potential vulnerabilities related to CVE-2019-18276.

Addressed potential vulnerabilities related to CVE-2021-44225.

Addressed potential vulnerabilities related to CVE-2021-36730.

Addressed potential vulnerabilities related to CVE-2022-22576 and CVE-2022-27778.

Addressed potential vulnerabilities related to CVE-2022-1292 and CVE-2022-2068.

Bug Fixes

Location (GX450 only)	
	Resolved an issue where location reports to servers configured by FQDN failed after upgrading to 4.9.6.
	Resolved an issue where Device ID was not reported correctly in user-defined NMEA sentences.
AMM	
	Updated MSCI certificates.
SNMP	
	Fixed write access from SNMP for GPIO configuration, adding an enhancement that modifying GPIO configuration requires authentication.
VPN	
	Resolved a potential issue with OpenVPN certificates being rejected by changing the default value for certificate validation to “Key Usage/Extended Key Usage”.

Known Issues

ACEmanager	
	The Radio Passthru button (located at Admin > Radio Passthru) does not work in Chrome or Edge browsers. Radio Passthru functions normally when using Firefox (Version 100.0.2).
LAN	
	GX450: IP Passthrough does not work on the Dual Ethernet expansion card.