ALEOS 4.9.5 Release Notes

ALEOS 4.9.5 is for AirLink GX450 and ES450 gateways.

New Features

Radio Module Firmware	
	Updated firmware for the following radio modules: MC7304: • Generic: 05.05.78.00 MC7354: • Generic: 05.05.58.00 • Sprint: 05.05.63.01
Cellular	
	Added support for Blank APN to allow the AirLink device to connect to certain networks with a blank APN.
	Added a setting to allow or disallow IPv6 ping responses.
GPS	
	Added a new button, GNSS Reboot Watchdog, under Location. This feature disables GNSS-related reboots when the watchdog is disabled
VPN	
	Revised the Split Tunnel settings in ACEmanager. A new section, Out of Band Policies, allows you to control incoming or outgoing traffic through the public Internet when VPN tunnels are configured.
WAN	
	Changed WAN Ping Monitor minimum values, increased frequency of pings, and allowed configuration of number of pings.
Logging	
	Added the ability to download logs in a compressed format to optimize data usage.
	Added the ability to capture raw NMEA stream.
ACEmanager	
	After clicking Reset to Factory Default, the confirmation messages that appear indicate the Reset Mode you are using (Reset All, Preserve Core Settings, Preserve Only User Password).

Security Enhancements

General	
	Prevented reading files via the tcpdump -V command in iplogging.
	Prevented Reverse SSH from being used to proxy network traffic.
Security and CVE Vulnerabilities	
	To address CVE-2020-8782, added a warning banner to ACEmanager when AAF Development Mode is enabled.
	To address CVE-2019-11855, the RPC server is enabled only if AAF user password is set.
	Fixed potential buffer overflow issues to address the following: • CVE-2019-11848 • CVE-2019-11858
	Applied a patch to pppd to address the following: • CVE-2020-8597
	Removed expat to address the following: • CVE-2016-0718 • CVE-2016-5300 • CVE-2018-20843
	Removed packages to address the following: • CVE-2019-9498 • CVE-2019-9497 • CVE-2019-9496 • CVE-2019-9499 • CVE-2019-11555 • CVE-2016-10743
	Addressed the following: • CVE-2017-11108 • CVE-2017-12989 • CVE-2017-12990 • CVE-2017-12995 • CVE-2017-12997 • CVE-2018-10103 • CVE-2018-10105 • CVE-2018-14461 • CVE-2018-14462 • CVE-2018-14463 • CVE-2018-14464 • CVE-2018-14465 • CVE-2018-14466 • CVE-2018-14467 • CVE-2018-14468 • CVE-2018-14469 • CVE-2018-14470 • CVE-2018-14879 • CVE-2018-14880 • CVE-2018-14881 • CVE-2018-14882 • CVE-2018-16227 • CVE-2018-16228 • CVE-2018-16229 • CVE-2018-16230 • CVE-2018-16301 • CVE-2018-16451 • CVE-2019-15166 • CVE-2018-16300 • CVE-2018-16452

Updated openLDAP to 2.4.48 to address: • CVE-2017-17740 • CVE-2019-13565 • CVE-2019-13057
Addressed CVE-2018-0732.
Updated bash to version 5.0 to address potential vulnerabilities related to: • CVE-2016-7543 • CVE-2019-9924
Updated libtomcrypt to address potential vulnerabilities related to CVE-2016-6129.
Updated BusyBox to address potential vulnerabilities related to: • CVE-2018-20679 • CVE-2016-6301 • CVE-2019-5747
Updated curl to 7.65.3 to address the following: • CVE-2018-1000120 • CVE-2018-1000122 • CVE-2018-1000300 • CVE-2018-0500 • CVE-2018-16839 • CVE-2018-16842 • CVE-2018-1000301 • CVE-2018-1000121 • CVE-2019-5443 • CVE-2019-5481 • CVE-2019-5482

Bug Fixes

WAN/Cellular
Resolved an issue where IP passthrough over USB was not working.
Corrected behavior where IP Manager would stop sending periodic updates after some uptime. IP Manager now sends periodic updates correctly.
VPN
Resolved an issue causing IP source violation when using VPN failover.
Added support for full-tunnel operation on the Legacy IPsec implementation.
Resolved an issue where the gateway accepted unsolicited inbound traffic not in the Friend List when full tunnel was configured.

Serial	
	Resolved an issue where TCP PAD communication could become disabled during an outbound TCP PAD connection attempt. Inbound TCP PAD connection attempts during an outbound TCP PAD connection attempt are now terminated cleanly. As well, an invalid Destination Address of 0.0.0.0 will not result in an outbound TCP PAD connection attempt.
	Resolved an issue where Modbus ID 43 would result in an extra “0x2b” inserted in the Modbus stream.
	Resolved an issue where the firewall did not always allow USB PPP traffic on boot.
	Fixed an issue preventing AT Telnet from working properly when the gateway is configured for Reverse Telnet operation.
Ethernet	
	Fixed an issue preventing the MAC address from being displayed correctly in the Status > Ethernet field.
SMS	
	Added an SMS Message Format setting for selecting 3GPP or CDMA/3GPP2 message formats to suit certain carriers. The default message format from previous versions of ALEOS remains the default.
Dynamic DNS	
	Removed obsolete providers from the list of dynamic DNS providers.
Statistics	
	Resolved an issue with inconsistent reporting of bytes sent on cellular uplink.
AT Commands	
	Replaced the command AT*IPPING with a new AT command AT*IPPINGSEC to get and set the values of the test interval of the Ping Test and Traffic Monitor. The command accepts seconds instead of minutes.
	Resolved an issue where ERROR was returned when the text of an SMS sent by AT command included commas.
Event Reporting	
	Resolved an issue where two digital inputs being triggered together generated only one event report.
	Resolved an issue where SNMP trap events were not sent for Digital Input 5.
	Resolved an issue where the reported Bytes Sent value (Status > Cellular > Statistics) could reach maximum and reset to zero.
SNMP	
	Updated Sierra MIB to prevent errors when running a walk via SNMP.
ALMS	
	Resolved an issue where ALMS would reject an FQDN address for GPS Report Server 1 IP in the ALMS template.

Admin	
	Resolved an issue where negative temperatures of the radio module (-10 °C, for example) were being reported incorrectly.