ALEOS 4.4.5 Release Notes

The ALEOS 4.4.5 release is for the AirLink GX400, GX440, ES440, and LS300. Refer to the ALEOS Software Configuration User Guide for update instructions.

IMPORTANT NOTICE

Upgrading to this release will make the following configuration changes to the gateway:

- If **DMZ Enabled** is set to Automatic, and **Host Connection Mode** is not set to Ethernet Uses Public IP, **DMZ Enabled** will be disabled.
- The “viewer” account will be removed, and cannot be re-enabled.
- If the “sconsole” user was previously using the default password, the “sconsole” account will be disabled.
- If the user password is default, Telnet/SSH will be disabled on the WAN interface.
- If the user password is default, remote access to server-initiated MSCI will be disabled.

Customers using these features may need to re-enable them after the software update (except for the “viewer” account). Please read these release notes carefully before installing this release.

New Features

ACEmanager

The “viewer” user account has been removed.

The “sconsole” user account is now disabled by default.

- If the “sconsole” user was previously using the default password, the “sconsole” account will be disabled after upgrading.
- To enable the “sconsole” account, ALEOS requires the customer to set a password.

Added a new setting for Telnet/SSH Access Policy. Telnet/SSH can now be set to LAN+WAN, LAN only or Disabled (default). When upgrading a gateway to 4.4.5, if the user password is default, Telnet/SSH is disabled on the WAN interface.

Added a new setting for Server-Initiated MSCI. This setting is labeled “HTTP Server And ACEView Services” in ACEmanager. Server-Initiated MSCI can now be set to LAN+WAN, LAN only or Disabled (default). When upgrading a gateway to 4.4.5, if the user password is default, remote access to server-initiated MSCI is disabled.

Security

Secure firmware update ensures that all firmware images are authentic images from Sierra Wireless. The gateway will authenticate all received firmware bundles before installing them.

If DMZ Enabled is set to Automatic, and Host Connection Mode is not set to Ethernet Uses Public IP, DMZ Enabled will be disabled.

Improved randomness for session timer generation.

AT Commands

Before changing the user password with AT/ACEPW, you must enter the current password, using AT*ENTERCND.

General

Added a userspace monitor interface for YAFFS.

Made improvements to YAFFS block retirement algorithm.

Bug Fixes

Security

Resolved an issue where inbound port filtering rules were blocking forwarded ports to the host device.

Updated OpenSSL package to 1.0.2l to address potential vulnerabilities related to:

CVE-2016-0701	CVE-2017-3731	CVE-2016-2181
CVE-2016-0702	CVE-2017-3732	CVE-2016-2182
CVE-2016-0705	CVE-2016-2105	CVE-2016-2183
CVE-2016-0797	CVE-2016-2106	CVE-2016-6302
CVE-2016-0798	CVE-2016-2107	CVE-2016-6303
CVE-2016-0799	CVE-2016-2109	CVE-2016-6304
CVE-2016-0800	CVE-2016-2176	CVE-2016-6306
CVE-2016-2842	CVE-2016-2177	CVE-2015-3195
CVE-2015-1794	CVE-2016-2178	CVE-2015-3197
CVE-2015-3193	CVE-2016-2179	
CVE-2015-3194	CVE-2016-2180	

Updated Dropbear to address potential vulnerabilities related to CVE-2017-9078 and CVE-2017-9079.

Updated tcpdump and libpcap to address potential vulnerabilities related to CVE-2014-8769 and CVE-2014-8767.

Updated Linux kernel to address potential vulnerabilities related to CVE-2017-14106.

Addressed potential vulnerabilities related to CVE-2017-7520 and CVE-2017-7479 (OpenVPN).

Updated SNMP to address potential vulnerabilities related to CVE-2015-5621.

Updated Linux kernel to address potential vulnerabilities related to CVE-2014-7822.

Updated Linux kernel to address potential vulnerabilities related to CVE-2014-9888.

Updated Linux kernel to address potential vulnerabilities related to CVE-2015-3288.

Updated libcurl to address potential vulnerabilities related to CVE-2016-5421.

Added additional user input validation to resolve CVE-2017-15043.

Addressed potential vulnerabilities related to CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496 (dnsmasq) (see https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00006.html)