ACM 2.1 Release Notes

ACM 2.1 provides a new load balancing/failover feature for MG90 routers, and addresses security vulnerabilities.

The ACM 2.1 release includes both FIPS and non-FIPS versions.

ACM 2.1 is strongly recommended for all existing ACM customers.

Upgrade Requirements

Important: *Upgrade to ACM 2.1 can only be performed from ACM 2.0 or ACM 1.6. Customers on previous ACM releases must first upgrade to ACM 1.6, and then upgrade from ACM 1.6 to ACM 2.0.1.*
Note—Upgrade can only be performed for the same ACM SKU (FIPS or non-FIPS).

ACM 2.1 can also be installed as a new instance (not upgrading from a previous ACM version) and the previous version's configuration components can be ported over.

Supported Embedded Software Versions

The ACM 2.1 (FIPS and non-FIPS) Release is supported on the following configurations:

Embedded software	Platform supported
MGOS 4.3	MG90
MGOS 3.15	oMG500/oMG2000
ALEOS 4.12	MP70, LX60, RV50, RV55
ALEOS 4.9.x	GX450 (and prior)
Tested with NCP 10.13	NCP Secure Entry Client

Server Platform Support

ACM 2.1 has been tested on:

- Dell R240XL server
- VM running on VMware vSphere 6.5 (ESXi 6.5)

Note: ACM 2.1-FIPS is FIPS-compliant and meets the requirements of the Federal Information Processing Standard 140-2, security level 1 (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2164.pdf).

© 2019 Sierra Wireless. All rights reserved.

New Features

Dynamic DNS

ACM 2.1 introduces Dynamic DNS (DDNS) support as a high availability load-balancing/failover configuration method for AirLink MG90 routers running MGOS 4.3.

Addressed Issues

Security

Addressed security issues (apt)

CVE	Severity
CVE-2019-3462	High

Addressed security issues (bash)

CVE	Severity	CVE	Severity
CVE-2014-6271	Critical	CVE-2014-6278	n/a
CVE-2019-9924	High	CVE-2014-7169	n/a
CVE-2016-9401	Medium	CVE-2014-7186	n/a

Addressed security issues (busybox)

CVE	Severity
CVE-2019-5747	High

Addressed security issues (curl)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2016-8619	Critical	CVE-2016-8623	High	CVE-2016-3739	Medium
CVE-2016-8620	Critical	CVE-2016-8625	High	CVE-2016-8616	Medium
CVE-2018-16839	Critical	CVE-2018-1000121	High		
CVE-2018-16842	Critical	CVE-2019-5443	High		
CVE-2018-1000007	Critical				
CVE-2018-1000120	Critical				
CVE-2018-1000122	Critical				
CVE-2018-1000301	Critical				

Addressed security issues (hostapd)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2019-9497	High	CVE-2017-13077	Medium	CVE-2019-9495	Low
CVE-2019-9498	High	CVE-2017-13078	Medium		
CVE-2019-9499	High	CVE-2017-13079	Medium		
		CVE-2017-13080	Medium		
		CVE-2017-13081	Medium		
		CVE-2019-11555	Medium		

Addressed security issues (libxml2)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2016-4448	Critical	CVE-2016-1833	Medium	CVE-2015-5312	n/a
CVE-2016-4658	Critical	CVE-2016-1836	Medium	CVE-2015-7499	n/a
CVE-2017-7376	Critical	CVE-2016-1837	Medium	CVE-2015-7500	n/a
		CVE-2016-1838	Medium	CVE-2015-8035	n/a
CVE-2016-1762	High	CVE-2016-1839	Medium	CVE-2015-8242	n/a
CVE-2016-1834	High				
CVE-2016-1840	High				
CVE-2016-4447	High				
CVE-2016-5131	High				

Addressed security issues (lighttpd)

CVE	Severity
CVE-2008-4359	n/a
CVE-2008-4360	n/a

Addressed security issues (ntp)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2019-8936	High	CVE-2016-2519	Medium	CVE-2014-9295	n/a
		CVE-2016-9310	Medium	CVE-2014-9750	n/a
		CVE-2016-9311	Medium	CVE-2014-9751	n/a

Addressed security issues (openssh)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2016-1908	Critical	CVE-2016-3115	Medium	CVE-2015-5352	n/a
				CVE-2015-5600	n/a
CVE-2015-8325	High			CVE-2015-6563	n/a
CVE-2016-6515	High			CVE-2015-6564	n/a
CVE-2016-10708	High				

Addressed security issues (openssl)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2016-1908	Critical	CVE-2016-6210	Medium	CVE-2018-0739	Medium
		CVE-2016-7055	Medium	CVE-2018-5407	Medium
CVE-2016-6515	High	CVE-2016-10011	Medium	CVE-2018-15473	Medium
CVE-2016-8858	High	CVE-2017-3735	Medium	CVE-2018-20685	Medium
CVE-2016-10009	High	CVE-2017-3736	Medium	CVE-2019-1559	Medium
CVE-2016-10010	High	CVE-2017-3737	Medium	CVE-2019-6109	Medium
CVE-2016-10012	High	CVE-2017-3738	Medium	CVE-2019-6111	Medium
CVE-2017-3731	High	CVE-2018-0734	Medium		
CVE-2018-0732	High	CVE-2018-0737	Medium	CVE-2015-6563	n/a
				CVE-2015-6564	n/a

Addressed security issues (perl)

CVE	Severity	CVE	Severity
CVE-2018-6913	Critical	CVE-2018-12015	High
CVE-2018-18311	Critical		
CVE-2018-18312	Critical		
CVE-2018-18313	Critical		
CVE-2018-18314	Critical		

Addressed security issues (python)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2016-5636	Critical	CVE-2018-1060	High	CVE-2016-0772	Medium
CVE-2017-1000158	Critical	CVE-2018-1061	High	CVE-2016-5699	Medium
		CVE-2018-14647	High		
		CVE-2019-13404	High		

Addressed security issues (strongswan)

CVE	Severity	CVE	Severity
CVE-2017-11185	High	CVE-2018-5388	Medium
CVE-2018-10811	High		
CVE-2018-16151	High		
CVE-2018-16152	High		
CVE-2018-17540	High		

Addressed security issues (systemd)

CVE	Severity	CVE	Severity	CVE	Severity
CVE-2018-15686	Critical	CVE-2018-16864	High	CVE-2018-1049	Medium
CVE-2018-15688	Critical	CVE-2018-16865	High	CVE-2018-15687	Medium
		CVE-2019-3842	High		

Addressed security issues (util-linux)

CVE	Severity
CVE-2017-5191	Medium

Known Issues

Dynamic DNS (DDNS)

If a network issue interrupts communication between ACMs in the DDNS cluster, the DNS data for a small number of connected gateways (~5%) may temporarily be incorrect.

The affected data recovers when IPsec tunnels change state.

Sierra Wireless Contact Information

Sales information and technical support, including warranty and returns:

Web: sierrawireless.com/company/contact-us/

Global toll-free number: 1-877-687-7795

Corporate and product information: sierrawireless.com