Addendum Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Special Build 8.5.182.11

Base Code: 8.5.182.0
Special Build: 8.5.182.11

8.5 MR8 Escalation Release

Image name	MD5	Comments
AIR-CT5500-AP_BUNDLE-K9-8-5-182-11.aes	11251ac6a07941097f52d806b2455f2c	Cisco Wireless Controller AP Bundle Software for 5508 Platform
AIR-CT5500-K9-8-5-182-11.aes	6e2be0c28bf78bf81b355a9c95043497	Controller Image for 5508 Platform
AIR-CT5520-K9-8-5-182-11.aes	ee2c74043384dfd24ef05f5a056e66b1	Controller Image for 5520 Platform
AIR-CT8540-K9-8-5-182-11.aes	ee2c74043384dfd24ef05f5a056e66b1	Controller Image for 8540 Platform
AIR-CT8500-K9-8-5-182-11.aes	ee2c74043384dfd24ef05f5a056e66b1	Controller Image for 8510 Platform
AIR-CT7500-K9-8-5-182-11.aes	ee2c74043384dfd24ef05f5a056e66b1	Controller Image for 7510 Platform
AIR-CT3504-K9-8-5-182-11.aes	531bd658b6a5e40050f4d500018ee393	Controller Image for 3504 Platform
AIR-CTVM-K9-8-5-182-11.aes	1d75dea384f9139b6b1291d1004b24ab	Virtual Controller Image for Small Scale Deployment
AIR_CTVM_LARGE-K9_8_5_182_11.aes	13d754c21c362c333dd550860b566793	Virtual Controller Image for Large Scale Deployment
ap1g4-ME-k9w8-tar.8-10-185-11	d4b3b7c9fc35e6536af314110ea09645	1850 Mobility Express Software
ap1g5-ME-k9w8-tar.8-10-185-11	ec0c8e914e858f308fe745abb35834a8	1815 Mobility Express Software
ap3g3-ME-k9w8-tar.8-10-185-11	f4178c6fed7ebdf2c3624fc8c3041210	2800, 3800 Mobility Express Software
ap_bundle_8.5.182.11	7a4f4bebdbe26e7e2ab59963cb13bfd5	Mobility Express Bundle Software

8.5.182.11 is an Escalation build published from the 8.5.182.0 CCO image and it is an engineering special that resolves the following additional caveat(s):

8.5.182.11

CSCwf67316	2800/3800/4800/1560/IW6300 may not detect radar on the required levels after CAC time. See Field Notice
CSCwc81656	AIR-CAP2702E-K-K9 Flash File System Corruption
CSCwa40778	Cisco Wireless LAN Controller AireOS Software FIPS Mode Denial of Service Vulnerability
CSCwc61122	Cisco Access Point Software Denial of Service Vulnerability
CSCwc70131	Cisco Access Point Software Command Injection Vulnerability
CSCwd80290	IOS AP image validation certificate Failed/Expired; causing AP join issues. See Field Notice
CSCvz99036	Cisco Access Points VLAN Bypass from Native VLAN Vulnerability
CSCvz84912	8540 WLC crash with Task Name: Dot1x_NW_MsgTask_5, Reason: System Crash
CSCvv03641	After AP SSO, few APs teardown DTLS and connect back to the controller

Americas Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

ENGINEERING SPECIAL USE DISCLAIMER

The Engineering Special fix supplied herewith is a Temporary Software Module which has undergone limited testing. This temporary software module is provided “AS-IS” without warranty under the terms of the END USER LICENCSE FOR THIS PRODUCT. Please use this software at your own risk. The intention for this code fix is for you to use in your production environment until a released version is available.

This code is supported by the TAC organization. Please report all comments, suggestions, and problems about this code directly to wnbu-escalation@cisco.com. If you are satisfied with the solution, please inform the alias.

Contact wnbu-escalation@cisco.com with any questions.

Americas Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA