FW Version: 4.5.0.2

Published Date: 2016-12-08

Copyright © 2016

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

Content:

Revision History and System Requirement:

Firmware Version	Date	Model Hardware	History
4.5.0.2	08 Dec 2016	DWC-2000/A1	Bug fixes and enhancement
4.4.0.3	20 May 2015	DWC-2000/A1	Bug fixes and enhancement

Firmware Details:

Image Version	HW	MD5 Checksum
DWC-2000_A1_FW_4.5.0.2_WW	A1	d615ac9b2a0935377c3d2d9e32eafb75

Important Notes:

1. GNU/Linux Bash Shell vulnerability (CVE-2014-6271)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since these devices do not expose the shell interface through CLI nor WEB interface (including CGI).
Reference website:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

http://seclists.org/oss-sec/2014/q3/650

https://blogs.akamai.com/2014/09/environment-bashing.html

2. SRTP Memory Leak (CVE-2014-3513)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since these devices do not support SRTP and based on OpenSSL 1.0.x versions.
Reference website:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3513

3. Build option no-ssl3 is incomplete (CVE-2014-3568)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since the existing code base, we do not configure build option to no-ssl3.

Reference website:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3568

Notes for Configuration Auto-Backup/Restore in USB Storage:

D-Link DWC Unified Controller support configuration backup or restore automatically while a USB drive is inserted. Following information instructs what condition will perform backup/restore.

1. The configuration will be automatically backed up to the USB drive as soon as the USB drive is inserted. The back name has format <Model Name>_<Serial Number>.cfg provided this USB drive doesn't have a backup configuration file from a DWC already present.

2. The system LED on the DWC blinks 3X in amber to indicate a backup operation has started.

3. The configuration in the USB drive can be updated if the user manually clicks 'Save Settings' in any GUI page and provided the Model Number and the Serial Number of the DWC matches with the file already present in the USB drive.

4. In case of reboot, the DWC checks for the presence of configuration file (with format ModelName_SerialNumber.cfg). If found, the configuration from the USB drive is restored on the DWC. If a configuration file with the correct format is present in both connected USB drives, the configuration from the first USB drive will be used to restore the DWC.

5. The USB drive can have only one configuration with the above mentioned format for each model name.

6. If the USB drive is plugged in to the DWC which is in factory default state, then during reboot, no backup is taken since no custom configuration file exists in the DWC by that time. The custom configuration is stored on the USB drive once the user clicks Save Settings in any GUI page.

Upgrading Instructions:

Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *DWC-2000 User Manual ver. 1.00.*

New Features:

Firmware Version	New Features

4.5.0.2	1. DWL-8710AP Support 2. Multiple LDAP SSID Mapping Enhancement 3. Hotspot enhancement changes 4. AP firmware upgrade enhancement. 5. New Dashboard and Wizard feature set.
4.4.0.3	1. Re-name FW 4.4.0.2_B701 to v4403. 50977 - DHCP class B support needed to be added . 51044 - Multicast to unicast and dhcp to unicast support for AP profile radio 51049 - Session Time Out support for captive portal users (local user db) 51053 - Billing and Temp Users GUI optimization in DWC-2k

Problems Fixed:

Firmware Version	Problems Fixed
4.5.0.2	1. Unable to delete/deactivate the licenses through CLI HQ20130426000004 2. OpenSSL Vulnerability Change Cipher 3. Device is vulnerable to SQL injection attack for cookie. 4. Device is vulnerable with SRTP Memory Leak (CVE-2014-3513) 5. Not able to perform trace route or ping functionality of ipV6 addresses from diagnostics page HQ20141104000020 6. Need enable 80Mhz for Mexico 7. WLAN IP address display 10.90.90.90 8. Observed critical error after STA pass captive portal Login in IE11 browser(DWC-1000) HQ20150204000014 9. Unable to open the GUI/frontdesk page of DWC-2000 device when it is connected to DSR device in NAT mode HQ20150324000017 10. Observed critical error in the IE 11 browser when user refreshes CP window. 11. Eliminate the double quote for WPA/WPA2 key in the "print ticket" of DWC-1000 device HQ20150518000017 12. Observed critical error in discovered ap page when we add large ip range HQ20150804000021 13. WEP security mode is not persisting after reboot for the default vap ssid's in dwc-2k 14. Upper level channels are not displaying in 5GHz radio for all countries.

15. When changing the radio Primary Channel from lower to upper then bandwidth is also getting effected from 40 to 20 HQ20150907000008

16. IN CLI and in status dashboard memory utilization values should have unit MB not KB HQ20150930000015

17. Enable redirect functionality not working on mobile devices when CP type as SLA HQ20151006000015

18. DWC-2000: Device is vulnerable to CSRF attack.

19. Channels list in managed ap page, in status managed ap page channel list pages are different from ap profile radio page HQ20150701000015

20. User is able to add the ip address in the DHCP pool which is alredy configured in the DHCP reserved IP page HQ20150810000022

21. license activation page is not working in Localization branch

22. Able to save diff serv policy with diff serv class which doesn't have a match selector HQ20141110000017

23. Need to apply the patch for Multiple Vulnerabilities#CVE-2015-3195

24. Wireless configuration is not persisting some time

25. Unable to open DWC-1000 GUI pages when device is behind NAT with Port forwarding Rule HQ20151221000015

26. Force roaming option is getting disabled after reboot for managed ap entry added in valid access points page HQ20160106000002

27. Static key is being used for SSH Communication.

28. critical error in managed ap page HQ20151216000013

29. Ignore Broadcast option need to be removed from cli for ssid configuration

30. When both the radio of peermanaged ap is off then channel is not getting updated in master HQ20160201000019

31. Need to add test build patch for the "High CPU utilization issue"

32. Observed 500 Internal Server error with customer configuration file HQ20160127000016

33. Able to configure CP type [SLA/Permanent/Temporary] for the Control VLAN from CLI HQ20160201000014

34. Spelling mistake in pay pal configuration page. HQ20160218000017

35. LAN related logs are not coming in DWC-2000 HQ20160126000017

36. Need to add port 443 for remote management and ssl vpn

37. SSL/TLS use of weak RC4 cipher-CVE-2013-2566

	38. DWC-2000 M2 : Increase the MAC Auth database limit to 2048 39. Cavium glibc "Skeleton Key" Vulnerability Notification – CVE 2015-7547 40. The managed APs location information will be incorrectly overwritten. DBG14070102 41. [DWC] WDS link status and statistics pages are showing incorrect radio modes for the WDS connection in DWC-2000 DBG15100075
4.4.0.3	1. [HQ20150409000007] Channel information incorrect on Managed AP page 2. [HQ20150127000021] Auto Channel in 5G not work properly[DUSA20150122000002-USA] 3. [HQ20150323000013] Authorize.net for paid SLA isn't working for client installation[DUSA20150320000003-Canada] 4. [HQ20150402000018] Firmware problem 5. [HQ20150407000016] Unable to delete some users from DB[DRU20150406000005-Middle East] 6. [HQ20150409000010] We can add new vlan id to poll list via MIB browser (wsL2DiscoveryVlanRowStatus), even this vlan id not existed on clan list. 7. [HQ20150410000004] Does DWC-2000 support QoS Differentiated Services?

Tracking Issues:

Firmware Version	Tracking Issues (The potential fix has not been confirmed by customer or OBU)
N/A	N/A

Known Issues:

Firmware Version	Known Issues

4.5.0.2	DBG16120072-Cannot form cluster after uploading the customer's settings. DBG16120077-The WiFi-channel won't follow what we set in the controller. DBG16120024-DWC-2000_CLI_Vlan setup via CLI not work DBG16110379-DWC-2000_IP-ACL_The service of the IP-ACL issue DBG16110376-Cannot add user through CSV DBG16110307-The incorrect WEB UI of DWC-2000 DBG16110292-difference in alert message usage and actual usage left for temp CP

Related Documentation:

- DWC-2000 User Manual ver.1.00
- DWC-2000 CLI Reference Guide ver. 1.00