Firmware Version: V2.17.01
Prom Code Version:
Published Date: 2018/07/19

Content:

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
V2.17.01	2018/07/19	DCS-932L	B1,B2
V2.16.08	2018/05/15	DCS-932L	B1,B2
V2.14.04	2016/10/08	DCS-932L	B1,B2
V2.13.15	2016/7/20	DCS-932L	B1,B2
V2.12.01	2015/10/22	DCS-932L	B1,B2
V2.11.03	2015/9/1	DCS-932L	B1,B2
V2.10.03	2015/6/29	DCS-932L	B1
V2.01.03	2015/2/6	DCS-932L	B1
V2.00b6	2014/7/2	DCS-932L	B1

Upgrading Instructions:

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the D-Link website. The file is in .bin file format.
2. Log-in camera web UI and enter setup/Maintenance/Firmware upgrade
3. Click Browse… and specify the firmware file.
3. Click Upgrade. The camera starts to upgrade and will reboot automatically when the upgrade completes.

New Features:

Firmware Version	New Features
V2.17.01	1. Upgrade mydlink agent to 2.2.0-b33n. 2. Update ActiveX and Java Applet signing certificate
V2.16.08	1. Upgrade mydlink agent to 2.2.0-b33. 2. Change the default system time to 2018-01-01 3. Update the ActiveX and Java Applet with renewed code-signing certificate (validity period of the certificate is from 9/30/2016 to 10/1/2019). 4. Support digest authentication for Web UI (Cannot support basic authentication for Web UI) 5. Upgrade MatrixSSL to v3.9.3 that resolve the vulnerabilities in MatrixSSL 6. Add XSS protection mechanism for CGI command
V2.14.04	1. Upgrade mydlink agent to 2.1.0-b41.
V2.13.15	1. Upgrade mydlink agent to 2.1.0-b27.

	2. Change the HTTPs self-signed certificate to SHA2 algorithms. 3. Support Mydlink UID mechanism (mdb get dev_uid) 4. Change the support page hyperlink of Firmware Upgrade web-UI to www.dlink.com. 5. Updated OpenSSL to v0.9.8o. 6. Remove mDNSResponder daemon on the unit. 7. Remove the Bonjour settings from the Network Setup web-UI. 8. Change the default system time to 2016-01-01 9. Update the years in the copyright statement for IP Camera's web-UI to 2016. 10. Add authentication to CGI /config/stream_info.cgi. 11. Offer the password validation on console port. (Console's Password is synchronized with the admin's password)
V2.12.01	1. Update mydlink agent to v2.0.19-b54n. 2. The ActiveX and Java Applet signing certificate are updated.
V2.11.03	1. Update mydlink agent to 2.0.19-b54 2. Add the denoise mechanism to reduce the background noise 3. Add the login check mechanism to solve Brute Force Attack issue 4. Add Hardware Version item on the Status page of the camera's web-GUI. 5. Change the model and model number of the UPnP properties. F/W V2.11.03 only supports D-ViewCam version as below or above. 1. DCS-100 V3.6.5 + DP V1.6.13 2. DCS-100 V4.0.4 + DP V2.0.15
V2.10.03	1. Update mydlink agent to v2.0.19-b35. 2. Support auto image setting switching mechanism for H/W B1 and B2 (or above) camera lens. (*H/W B2 or above only supports v2.10.03 or above)
V2.01.03	1. Upgrade mydlink agent to v2.0.18-b61 2. Remove SSL, change to support TLS.
V2.00b6	Initial version. F/W v2.00 is not backward compatible to H/W Ax version.

Problems Fixed:

Firmware Version	Problems Fixed
V2.16.08	1. Fixed WPA2 vulnerability issue. 2. Fixes Cross Site Request Forgery (CSRF) vulnerability for FTP setting. 3. Fixes denial of service (DoS) vulnerabilities for upload firmware and restore configuration. 4. Remove crossdomain.xml to fix a security vulnerability issue. 5. Fixed a command injection issue in the change admin's password

	configuration (/setSystemAdmin). 6. Fixed the issue where sending long password on password field of html page.
V2.14.04	1. Fixed an issue that Mydlink service will be off line when FW upgrade to v2.13.15.
V2.13.15	1. Fixed CSRF vulnerability for the camera's web-UI (Exclude CGI APIs). 2. Fixed the "RSA-CRT key leaks" vulnerability. 3. Fixed the "LANDAP stack overflow" vulnerability. (discovered by search SEARCH-LAB) 4. Remove the "Arbitrary file upload interface" vulnerability. (discovered by search SEARCH-LAB) 5. Fixed an issue that Time zone setting for Minsk should be GMT+3. 6. Fixed a vulnerability - Authenticated Arbitrary File Upload with Root Privileges. (discovered by IOActive Security) 7. Fixed a vulnerability - Authenticated Root OS Command Injection in File Upload. (discovered by IOActive Security) 8. Fixed an XSS vulnerability - Stored XSS in User Name. (discovered by IOActive Security) 9. Fixed an XSS vulnerability - Reflected XSS in HTTP Host Header. (discovered by IOActive Security)
V2.11.03	1. Fixed the IE11 compatibility issue in Windows 10. 2. Change WPS LED behavior blinking time on WPS error/timeout to 10 seconds. 3. Remove the reboot function by pressing and holding the reset button in less than 3 seconds. 4. Add the pop-up warning message when the user creates an existing user account on Device Web GUI. 5. Support to auto-create FTP folder if the folder doesn't exist on FTP server.
V2.10.03	1. Fixed HTTPS issue that causes Day/Night control not work from portal/app. 2. Fixes the issue in which IP Cam cannot create FTP folder with FTP server on Netgear R7000 Router. 3. Fixed CGI /reset.cgi reboot command not work issue. 4. Modify Time Zone Table list to support some existing time zones changes.

Known Issues:

Firmware Version	Known Issues
V2.16.08	1. When firmware upgrade from v2.14 (or before) to v2.16, the webUI redirect

	will be failure. This is because the webUI authentication mode changes to Digest (brute-force intrusion)

Related Documentation:

N/A