



Firmware Version: V1.07.01
Prom Code Version:
Published Date: 2019/6/17

Content:

Upgrading Instructions:..... 2

New Features:..... 2

Problems Fixed: 3

Known Issues: 4

Related Documentation: 4

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
V1.07.01	2019/6/17	DCS-934L	A1,A2,A3
V1.06.02	2019/2/18	DCS-934L	A1,A2,A3
V1.05.04	2016/10/18	DCS-934L	A1,A2,A3
V1.04.15	2016/7/20	DCS-934L	A1,A2,A3
V1.03.01	2015/10/22	DCS-934L	A1,A2,A3
V1.02.05	2015/9/2	DCS-934L	A1,A2
V1.01.03	2015/2/6	DCS-934L	A1
V1.00_b2	2014/12/9	DCS-934L	A1

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
V1.07.01	<ol style="list-style-type: none"> 1. Upgrade mydlink agent to v2.0-b65 2. Change the default system time to 2019/01/01.
V1.06.02	<ol style="list-style-type: none"> 1. Upgrade mydlink agent to v2.2.0-b33 2. Change the default system time to 2018-01-01 3. Support digest authentication for the Web GUI (Cannot support basic authentication for Web UI) 4. Update the ActiveX and Java Applet with renewed code-signing certificate.
V1.05.04	<ol style="list-style-type: none"> 1. Upgrade mydlink agent to 2.1.0-b41.
V1.04.15	<ol style="list-style-type: none"> 2. Upgrade mydlink agent to 2.1.0-b27. 3. Change the HTTPs self-signed certificate to SHA2 algorithms. 4. Support Mydlink UID mechanism (mdb get dev_uid) 5. Change the support page hyperlink of Firmware Upgrade web-UI to www.dlink.com. 6. Updated OpenSSL to v0.9.8o.

	<ul style="list-style-type: none"> 7. Remove mDNSResponder daemon on the unit. 8. Remove the Bonjour settings from the Network Setup web-UI. 9. Change the default system time to 2016-01-01 10. Update the years in the copyright statement for IP Camera's web-UI to 2016. 11. Add authentication to CGI /config/stream_info.cgi. 12. Offer the password validation on console port. (Console's Password is synchronized with the admin's password)
V1.03.01	<ul style="list-style-type: none"> 1. Update mydlink agent to v2.0.19-b54n. 2. The ActiveX and Java Applet signing certificate are updated.
V1.02.05	<ul style="list-style-type: none"> 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. Support auto image setting switching mechanism for H/W A1 and A2 (or above) camera lens. (*H/W A2 or above only supports v1.01.03 or above) 6. Change the model and model number of the UPnP properties. F/W V1.02.05 only supports D-ViewCam version as below or above. <ul style="list-style-type: none"> 1. DCS-100 V3.6.5 + DP V1.6.13 2. DCS-100 V4.0.4 + DP V2.0.15
V1.01.03	<ul style="list-style-type: none"> 1. Upgrade mydlink agent to v2.0.18-b61 2. Remove SSL, change to support TLS.
V1.00_b2	1 st version

Problems Fixed:

Firmware Version	Problems Fixed
V1.07.01	<ul style="list-style-type: none"> 1. Fix an authenticated buffer overflow vulnerability issue.
V1.06.02	<ul style="list-style-type: none"> 2. Fixes the issue that Cross Site Request Forgery (CSRF) vulnerability for FTP setting. 3. Fixes the issue that denial of service (DoS) vulnerabilities for upload firmware and restore configuration. 4. Remove crossdomain.xml to fix a security vulnerability issue. 5. Upgrade MatrixSSL to v3.9.3 that resolve the vulnerabilities in MatrixSSL. 6. Fixed a command injection issue in the change admin's password configuration (/setSystemAdmin). 7. Fixed the issue where sending long password on password field of html page. 8. Fixed for WPA2 KRACK Vulnerabilities.

	<ul style="list-style-type: none"> 9. Fixed an issue that when set motion sensitivity to 0%, the motion alarm still occurs. 10. Remove GPL v3 open source (change open source used for e-mail function) 11. Add XSS protection mechanism for CGI command.
V1.05.04	<ul style="list-style-type: none"> 1. Fixed an issue that Mydlink service will be off line when FW upgrade to v1.04.15.
V1.04.15	<ul style="list-style-type: none"> 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 vulnerability - Authenticated Arbitrary File Upload with Root Privileges. (discovered by IOActive Security) 7. Fixed 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)
V1.02.05	<ul style="list-style-type: none"> 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.

Known Issues:

Firmware Version	Known Issues
V1.06.02	Block the webUI to access in Safari 12 because of no support Safari 12

Related Documentation:

N/A