Merit LILIN Technical Support Document

Document Number: Q000126
Date: 8/15/2016
Dept: Technical Support, Taipei

Subject: New security improvements for LILIN IP cameras and NVRs

1. CGI is protected for preventing inserting user authentication including DDNS, SNMP, SIP, Samba service.
2. Hardcoded username and password of web page is removed and encrypted.

In order to add extra security protection, the following protocols and mechanisms have been added to the recent firmware releases.

- HTTPs
- Digest authentication
- IP filters, black and white lists
- Password strength enforcement

LILIN will continuously improve security issues of LILIN IP cameras and NVRs if there is any and will soon add the followings:

- 802.1x
- Brute force attacks for account lock out for certain time
- HTTPs for LILIN DDNS
- Support HTTPs for LILINViewer
- Telnet will be disabled but can be enabled via web page.

Other Security Concerns

DDoS (A Distributed Denial of Service) & Botnet

NVRs or cameras could become DDoS & Botnet devices for attacking other Internet services. The root cause might be the camera developers use Internet open source for HTTP server and Telnet for cameras. LILIN wrote our own HTTP service and do not have default password for Telnet service.

SNMP

SNMP client is disabled by default.

UPnP

UPnP server is disabled by default.

Bonjour

Bonjour client is disabled by default.

FTP

FTP server is disabled by default.

HTTP

Some NVR and camera vendors have master password built-in in their devices. LILIN NVR and camera do not have default passwords built-in.

More Secure Way

LILIN P2P protocol is proprietary. LILIN P2P protocol is now available for LILIN NVR platform. LILIN P2P NVRs can be accessed by LILIN Navigator and LILINViewer.

Contact

Contact http://lilin.zendesk.com for technical support or any camera security issue found.