Date: 02/27/2020

Dear LILIN customers:

Thanks for using LILIN products. Recently discovered security vulnerabilities affect LILIN DVRs. LILIN rates these vulnerabilities with a CVSS v3.1 Base Score of 10.0 (Critical) and recommends customers to update the vulnerable DVRs with the fixed firmware immediately.

We apologize for any inconvenience caused to our customers. This document can further help LILIN's customers for understanding the consequences of the DVR's vulnerabilities and the actions LILIN has taken for improving product cybersecurity issues.

How many product lines affected
There are three firmware product lines affected that includes DHD5, DHD3, and DHD2 series.

Products were affected
The affected products modules are DHD516A, DHD508A, DHD504A, DHD316A, DHD308A, DHD304A, DHD204, DHD204A, DHD208, DHD208A, DHD216, and DHD216A.

There are total 13,062 DVRs sold.

Products were NOT affected
New released DVRs that includes DHD5104, DHD5216, and DHD5108 are NOT affected.

LILIN IP cameras series and NVR series are NOT affected

What are the vulnerabilities
The default credential for accessing the DVRs gets used for injecting script code for attacking other Internet devices.

1. DDoS attacks to other Internet devices.
2. Telnet gets opened by HTML CGI command.
3. PPPoE gets changed to DHCP.
4. Fixed host name injection issue for accessing NTP, FTP, DDNS, and MAIL servers.

What are the changes in the new firmware release
1. Force to change default username and password via user interface after firmware upgrade.
2. Validate legal string for the hostname of NTP server and FTP services for preventing injecting script code for attacking others.
3. Add encryption mechanism for preventing injection of any Linux script or command.

Actions taken by LILIN
- Publish vulnerability firmware fix on LILIN site.
- Disclosure product vulnerability at LILIN security bulletins.
- Find out where and whom that affected DVRs has been sold to from LILIN ERP and

MES system
- Sales call out LILIN branches, distributers, and installers for firmware fix issues.

Timeline
February 10, 2020: Qihoo 360 Technology Co. Ltd notified LILIN for vulnerabilities found.
February 10, 2020: LILIN replied for asking product codes and issues found.
February 12, 2020: LILIN identified the vulnerability and replied Qihoo for a fix.
February 14, 2020: LILIN published the fix and post solution on LILIN web site.

Other improvements by LILIN
We sincerely apologize about the inconveniences caused to our customers. In order to enforce product cyber security, LILIN has started to certify network products based on TAICS TS-0014-2 v2.0 via Taiwan Association of Information and Communication Standards (TAICS) in 2019.

LILIN will certify NVR/DVR series in early 2020 due to availability of TAICS TS-0014-3. LILIN also hires third-party Deloitte Taiwan and ETC (Electronics Testing Center, Taiwan) for vulnerabilities checking based on TAICS specification.

LILIN NVR 5 series has started complying with California IoT security law in Feb 2020.

LILIN P2, Z2, P3, Z3, P5, Z5, M, S, and Ultra series has started complying with California IoT security law in Feb 2020.

LILIN DHD5104, DHD5216, and DHD5108 are using encrypted firmware for preventing hackers from binwalk analysis.

LILIN NVR 3 and 5 series will use encrypted firmware in early Q2 2020 for preventing hackers.

LILIN has started to use RTSP over HTTPs for LILIN cameras and LILIN NVRs/DVRs (hybrid) in Feb 2020.

Again, we apologize for any inconvenience caused to our customers. If there is any question, feel free to contact LILIN sales worldwide for clarification.

Product Management Department
Merit LILIN Enterprise Co., LTD