Merit LILIN Application Note

LILIN Vulnerability Policy

Document Number：A00135
Date：2018/6/29
Dept: Technical Support, Taipei

1. Overview

LILIN are dedicated to protecting our customers against cyber security attacks on our network cameras, network video recorders & VMS products. LILIN regularly review, investigate, report & implement against cyber security vulnerabilities in our products.

LILIN's cyber security assurance team has been formed to manage cyber security threats throughout the lifecycle of its products; including design, development, verification, manufacturing and service phases. LILIN are constantly reviewing and enhancing our cyber security efforts to provide our valued customers with the highest quality, safe and reliable products.

LILIN cannot protect standardized network protocols and services from cyber-attacks, however we are committed to help minimize and prevent such events from occurring on LILIN products within our customers networks.

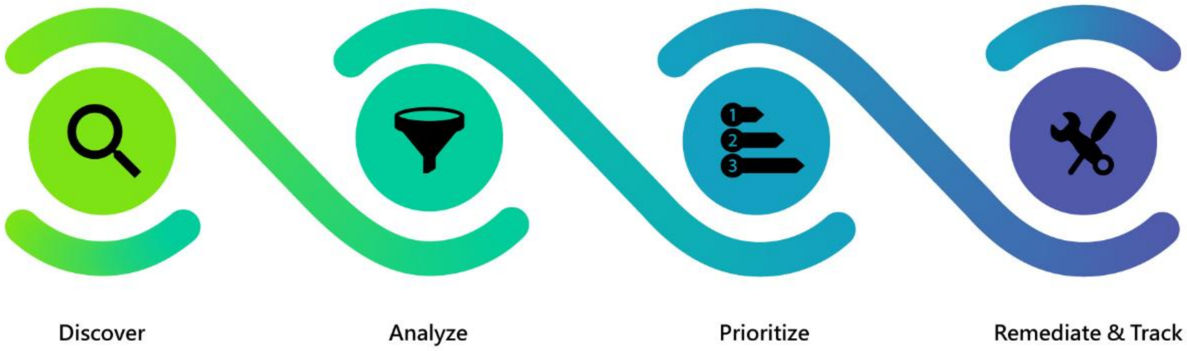
For the latest LILIN software and firmware updates, please visit this web site. The latest firmware fixes or software patches are maintained at the site.

2. Vulnerability management

LILIN are always working on maintaining the highest level of security for our products and customers. LILIN conducts product security maintenance throughout the product's life cycle.
In short, the vulnerability management is described below:

- Risk analysis and assessment of vulnerabilities with reference to the CVSS 3.0
- Security guidance throughout development by CIA-AAA (confidentiality, integrity, availability, authentication, authorization & accounting)
- Secure programming guidance and FIPS 140-2 for sensitive data protection & cryptography
- Vulnerability and open ports scanning in the testing phase
- Third-party vulnerability auditing for LILIN products by our security partner Deloitte Taiwan
- Security controls and checkpoints for software/firmware releasing, loading and storing

Based on the risks reported and discovered, we classify the severity of vulnerabilities as either critical or non-critical. The process for identifying a security vulnerability is discover, analyze, prioritize, remediate & track.



LILIN release firmware updates on a regular basis to address bug fixes and non-critical vulnerabilities that are found in our products. Occasionally, there may be a critical vulnerability discovered that leaves our devices vulnerable to attack. LILIN will focus its priorities to fix this issue immediately outside of the regular schedule and release a firmware fix for the vulnerable device.

3. Reporting suspected security vulnerabilities

We encourage and welcome you report any cyber security vulnerabilities found in LILIN products to help us to resolve & eliminate these threats. Please contact us at security@meritlilin.com.tw or raise a ticket at lilin.zendesk.com to report a vulnerability or other security concern.

LILIN will disclose and notify customers of any vulnerability found and of the resolution at LILIN Security Bulletins.

4. Response process

LILIN has established the Product Security Incident Response Team (PSIRT) committee to analyze all submissions of vulnerabilities to security@meritlilin.com.tw or lilin.zendesk.com.

LILIN PSIRT uses version 3.0 of the Common Vulnerability Scoring System (CVSS) as part of its standard process of evaluating reported potential vulnerabilities in LILIN products.

LILIN PSIRT will endeavor to reply within 72 hours & if needed, will ask questions to help in identifying a solution.

5. Receiving information from LILIN

LILIN have published this policy on LILIN Vulnerability Policy.

Subscribe to our product news and updates via the LILIN web site.

We also encourage users to take advantage of our many online resources:

- Subscribe to LILIN news.
- LILIN Downloads: With useful materials, such as brochures, firmware/software updates.
- LILIN Support: Report any support issue via lilin.zendesk.com.

6. Security third-parties

LILIN strive to provide our customers with the highest level of product security. To do so, LILIN have partnered with the third-party, Deloitte Taiwan, for product vulnerability auditing and checking. LILIN are also partnerded with TAICS for the latest network product security standards.

Deloitte.

TAICS

Contact
Contact lilin.zendesk.com for technical support.