Foscam's response to security flaws as reported by F-Secure (https://goo.gl/zMdzAY)

With regard to the security flaws mentioned in the F-secure reports, Foscam attributes great importance to it and arranged our Research and Development Department to analyze each of the items immediately.

After our analysis, below are following cases which will not influence customer's usage and product security:

1) Some cases mentioned do not exist, for example:
   a. ***"FTP server account uses empty password"***
      Customers can not log into FTP with empty password, which means customers are required to use accounts and passwords when they log into FTP.
   b. ***"Unauthenticated Remote Command Injection via Anonymous ONVIF SetDNS"***
      - *"Administrator Credential Disclosure via Anonymous ONVIF GetStreamUri"*
      - *"Unauthenticated Reboot via Anonymous ONVIF SystemReboot"*
      - *"Unauthenticated Persistent XSS via Anonymous ONVIF SetHostname"*

      These cases do not exist. Only with the administrator account can customers use them. And the administrator account is the account created by customer themselves with account ID and password.
   c. ***"Hidden Telnet functionality"***
      All device Telnet functionality is closed and cannot be activated.

2) Some cases could not happen because Foscam has already made enough protection
   a. ***"Non-random default credentials for web user interface account"***
      It's mandatory to change the user account and password before customers use Foscam device and the password should be more than 6 bits including numbers, letters and combination.
   b. ***"Missing restriction of multiple login attempts"***
      Foscam device has restriction that if multiple login attempts fail with 30 seconds, the device will be locked and cannot be logged in.

3) Some cases could happened only if with customers' administrator account information and customers are required to change their Foscam device's account ID and password
   a. ***"Configuration back-up file is protected by hard-coded credentials"***
      The configuration back-up file can only be got with administrator account, and even the files are got with the administrator account, the file is encrypted to make sure no information from it will be leaked.
   b. ***"Remote command injection in User Add"***
      Only with the administrator account can a User be added.

4) Below 2 cases only means when the IP camera is hacked on purpose, the IP camera will not show video properly, but the hacker is unable to obtain any user info.
    a. ***"Denial of service of the RTSP video feed"***
    b. ***"Buffer overflow in ONVIF SetDNS"***

Foscam really appreciates F-secure for their report, which helps Foscam to do better. Foscam will continue to optimize and strengthen our product security. A new firmware will be available soon to improve security, for example the disabled Telnet functionality will be removed and the protection ability to RTSP will be strengthened.

Foscam always attached great importance to our product security and we have a Security Department who are dedicated to improving our product security by delivering updated firmware on time. We thank all of you for the suggestions that can help us become better!