

Date: 09/02/15

To All iBaby Current and Future Family:

At iBaby, we strive to make our products deliver the best experience and service to our customers. We are a brand that cares about the safety of parents and their precious babies. Since 2011, we have served over 1000s of customers worldwide, without issues or complaints on security. The safety of our families is something that we take very seriously, and would never compromise under any circumstances. We are truly sorry for the misconception this has caused the public and we assure you that the following preventable measures have been executed to resolve the security issues and ensure the safety of our families:

- 1) The data communication between Apps and Cloud API is encrypted by AES and MD5.
(Encrypted data communication between Apps, Cloud and Monitor)
- 2) Enhanced the access token assignment method. Each access token will be destroyed after request completed.
- 3) The Cloud Server can block the hacker.
(Cloud Server can block the hacker replaying the data request what it captured.)
- 4) The alert file paths are encrypted and random; a serial number cannot be changed to obtain information from files.
- 5) HTTPS is enabled for the communication between Apps and Amazon Web Services.
(The alert file paths are encrypted and random, hacker will not be able to just change a serial number to get others' files. Also our monitors are hosted by Amazon Servers, therefore, the security is very high equivalent to military security.)

In addition, we recommend continuous password changes to your Wi-Fi router, not only for baby monitors, but also for any device connected to Wi-Fi. We also strongly suggest you to update your iBaby apps to the latest version to prevent future issues such as performance and server connection.

We'd like to take this opportunity to thank you for your time, which allows us to serve our families better.

With Love and Care,
iBaby Labs, Inc
Elnaz Sarraf
Vice President
+1 (650) 396-2436