

Release Note

Product Name: <FD836BA-HTV>
Release Version: <0106b>
Date: <2018/08/14>
Product Type ☒ Camera ☐ NVR ☐ Software

New Feature:

N/A

Changed Feature:

01. CGI and web UI no longer supports the following characters: \$, (,)

Bugs Fixed:

- | | |
|-----|---|
| 01. | Fixed CVE-2018-14769, CSRF(Cross-site request forgery) vulnerability. Mitigation by using User-Agent and referer to check and identify the source of request. * |
| 02. | Fixed CVE-2018-14770, allows authenticated users to execute arbitrary commands on a vulnerable version via ONVIF interface (/onvif/device_service). |
| 03. | Fixed CVE-2018-14768, allows authenticated users to execute arbitrary commands on a vulnerable version via update_lens.cgi. |
| 04. | Fixed CVE-2018-14771, allows authenticated users to execute arbitrary commands on a vulnerable version via eventsript.cgi. |
| 05. | Fixed failed to upload VADP package issue. |
| 06. | Fixed cannot set custom subnet mask in camera Network configuration page. |
| 07. | Fixed incorrect daylight saving flag causes VAST recording stop issue. |
| 08. | Fixed video frames sent have the same timestamp issue. |
| 09. | Fixed camera cannot change to day mode or night mode correctly due light sensor reading issue. |
| 10. | Fixed event log cannot be appeared correctly in VAST when profile motion 1~5 is triggered. |
| 11. | Replace insecure SHA1 certificates with SHA-2. |

* Please note that after updating to this firmware version you won't be able to use the browser to execute CGI commands to the camera. If you require to execute CGI commands from the browser, please temporarily disable the CSRF protection function (Configuration -> Security -> Miscellaneous -> uncheck "Enable Cross-Site Request Forgery(CSRF) Protection"). Be sure to change back the function as soon as the command has been executed.