

---

Product Name: <TB9330-E>  
Release Version: <0121d\_Beta2>  
Date: <2020/5/4>  
Product Type ☒ Camera ☐ NVR ☐ Software

---

## New Feature:

- N/A

## Changed Feature:

- Remove the customized script function on the event settings page.

## Bugs Fixed:

- Fixed CVE-2020-11949, Allow an authenticated user to obtain arbitrary files from a camera's local filesystem via testserver.cgi.
- Fixed CVE-2020-11950, Allow an authenticated user to upload and execute a script (with resultant execution of OS commands) via eventscript.cgi.

## Known Issue:

- If set recording to NAS, the content management will not display correct search result after reboot the camera and cyclic function will failed once there is no free space in NAS.
- If selecting "except lens configuration" to restore the camera, the Trend Micro IoT Security package will be deleted.
- In digest mode, users will need to login more than one time and may need to re-login when switching page.
- If you launch multi-tab to view camera streaming, it will display streaming on first tab and the rest will show black image.
- It will display black image once change the camera URL from http to https.
- The license expiration event of Trend Micro will probabilistic not works.

## Release Version: <0121d>

Date: <2020/02/25>

## New Feature:

- Support Bonjour.
- Support showing hostname on DHCP server.

## Changed Feature:

- Upgrade VADP version to 1.4.2.2.
- Upgrade Trend Micro package version to v1.2b.a1.7.3.

- Upgrade embedded Genetec version to v2.0.4.2.
- Upgrade plugin version to v2.0.0.7.
- Upgrade smartVCA package version to v6.4.3.7-2b.
- Support over-exposure. (Except FE/TB/MD series.)
- Support AE configuration adjust when WDR Pro enabled.\*
- Change the default authentication of streaming protocol from basic to digest.
- Change the HTTP protocol from supports HTTP/1.0 and HTTP/1.1 to HTTP/1.1 only.

## Bugs Fixed:

- Fixed CVE-2019-19936, remove and not support eventtask.cgi
- Fixed CVE-2019-14457, have stack overflow vulnerability via HTTP referer header.
- Fixed CVE-2019-14458, have denial of service vulnerability via HTTP host header.
- Fixed CVE-2019-14477 SACK Panic (Linux >= 2.6.29)
- Fixed CVE-2019-11478 SACK Slowness (Linux < 4.15) or Excess Resource Usage (all Linux versions)
- Fixed CVE-2019-11479 Excess Resource Consumption Due to Low MSS Values (all Linux versions).
- Enhanced error handling for input /cgi-bin/viewer/video.jpg with illegal parameters.
- Enhanced error handling for /cgi-bin/admin/setparam.cgi?network\_http\_port.
- Fixed an issue in which SD card playback on multiple web clients could cause playback fail.
- Enhanced the stability of firmware upgrade.
- Fixed an issue in which formatting SD card could cause other service fail.
- Enhanced SD card status display mechanism.
- Fixed zoom/focus bar incorrect issue.
- Fixed could not connect to camera via public IP once enable PPPoE.
- Fixed seamless recording not resuming the recording correctly issue.
- Fixed timeshift function not work issue.
- Fixed upgrade firmware failed in specific circumstance.
- Fixed cannot display webpage issue when connect to camera by using not default https port.
- Fixed the maximum exposure bar only support to 1/120 on 1080P 60FPS Mode.
- Fixed service name will return to default after upgrading firmware.
- Fixed PIR function not working.
- Fixed FD9189-HT pink image when setting as night mode and restore to factory default.
- Fixed the continuous recording clip of SD card will not show on the content management page.
- Fixed the recording cyclic fail and camera stop recording.

## Known Issue:

- In digest mode, users will need to login more than one time and may need to re-login when switching page.

- If you launch multi-tab to view camera streaming, it will display streaming on first tab and the rest will show black image.
- It will display black image once change the camera URL from http to https.
- The license expiration event of Trend Micro will probabilistic not work.

\* TB9330-Elf you manually upgrade the firmware to 0121d, please restore the camera to default. And the AE configuration will be displayed.

## **Release Version: <0113d>**

**Date: <2019/06/05>**

### **New Feature:**

- Support Trend Micro event.
- Support Stratocast.
- Support VIVOCloud.
- Support ONVIF OSD.
- Support Smart VCA.
- Support Smart Motion Detection.
- Support Standard VCA.

### **Changed Feature:**

- Upgrade ONVIF version to 18.06.
- Upgrade Web API to 0311d.
- Change the default access name for HTTP/RTSP stream format.
- Build in Genetec package version 1.0a.a0.3.2.

### **Bugs Fixed:**

- Fixed CVE-2019-10256, an authentication bypass vulnerability.
- Fixed VAST reconnect issue if set event recording in VAST.
- Fixed an issue in which upgrading firmware gets stuck after a certain operation of VADP.
- Fixed a lot of "unable to get data length from buffer" logs issue when enable motion detection.
- Fixed camera IP change to 127.0.0.1 issue after reboot when Stratocast is enabled.
- Fixed Genetec package crash issue when smart motion is enabled.

## **Release Version: <0109a>**

**Date: <2018/12/11>**

### **New Feature:**

- Support Trend Micro package.

- Support plugin-free streaming.
- Support shock detection.
- Support IR cut filter day/night mode could sync with multiple digital inputs.
- Support standard VCA package.
- Support Smart motion package.
- Added metering mode.
- Added deblur in scene mode.

## Changed Feature:

- Upgraded Web API to 0311b.
- Upgraded smart SD card version to 1.0.1.4.
- Remove "Customsafe100" from Configuration > Network > DDNS > Provider list.
- Change from pop-up window to notification when uploading configuration file.
- Disable CSRF mechanism after reset to factory mode and will be enable after setting password in factory mode.

## Bugs Fixed:

- Fixed CVE-2018-18244, persistent XSS via HTTP Referer header.
- Fixed CVE-2018-18005, DOM-Based XSS vulnerability in camera event\_script.js
- Fixed CVE-2018-18004, a notification will show on camera home page when hidden service has been enabled.
- Fixed an issue in which firmware upgrading gets stuck if turn on Trend Micro.
- Fixed Trend Micro display incorrect status in package management page.
- Fixed Trend Micro IoT Security incorrect status in Trend Micro setting page.
- Fixed Trend Micro current version become invisible after upgrade signature issue.
- Fixed failed to upload VADP package issue.
- Fixed root password cannot be set in factory mode.
- Fixed cannot set custom subnet mask in camera Network configuration page.
- Fixed an issue in which smart FPS works incorrectly when WDR Pro is enable.
- Fixed an issue in which NAS cyclic storage deletes all recordings, only the last day left.
- Fixed an issue in which IR adjustment may not work as expected while adjust angle.
- Fixed drop frame issue when WDR/Linear auto switch.
- Fixed AE hunting issue when set to WDR mode +0.7EV after reboot.

**Release Version: <0106b>**

**Date: <2018/08/22>**

**New Feature:**

- N/A

**Changed Feature:**

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

**Bugs Fixed:**

- 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. \*
- Fixed CVE-2018-14770, allows authenticated users to execute arbitrary commands on a vulnerable version via ONVIF interface (/onvif/device\_service).
- Fixed CVE-2018-14768, allows authenticated users to execute arbitrary commands on a vulnerable version via update\_lens.cgi.
- Fixed CVE-2018-14771, allows authenticated users to execute arbitrary commands on a vulnerable version via eventsript.cgi.
- Fixed event log cannot be appeared correctly in VAST when profile motion 1~5 is triggered.

\* 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.