Release Note

Product Name: < FD8377-HV>
Release Version: <0120c_SA2019002>
Date: <2019/09/09>
Product Type ☒ Camera ☐ NVR ☐ Software

New Feature:

- Support Bonjour.
- Support Trend Micro event.
- Support Trend Micro refund.
- Support showing hostname on DHCP server.

Changed Feature:

- Upgrade VADP version to 1.4.2.0.
- Upgrade ONVIF version to 18.12.
- Support setting multiple languages for host name, video title, etc.
- Users can download a specific time interval recording from SD card.
- Embedded Genetec protocol.
- Removed Genetec package.
- Removed DDNS forget key button.
- Change the default authentication of streaming protocol from basic to digest.

Bugs Fixed:

- Fixed CVE-2019-14457, Stack-based buffer overflow via a crafted HTTP header.
- Fixed CVE-2019-14458, Allow a denial of service via a crafted HTTP 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).
- Fixed no streaming via multicast issue when using Genetec Security center.
- Fixed an issue in which SD card playback on multiple web clients could cause playback fail.
- Fixed an issue in which formatting SD card could cause other service fail.
- Fixed an issue in which users can set http port to empty by CGI commend.
- Enhanced the stability of firmware upgrade.
- Fixed wrong fps information display in 3rd party software.

Known Issue:

- If the snapshot and log file is sent when the event trigger type is set to smart SD, users will not able to search them in Content management page.
- In digest mode, users will need to login more than one time and may need to re-login when switching page.
- If sending a file to the NAS event action, the NAS will not receive the file and the mounting

status might become Error.

Release Version: 0113b
Date: 2019/04/15
New Feature:
N/A
Changed Feature:
- Upgrade ONVIF version to 18.
- Upgrade Web API to 0311c.
- Upgrade Genetec package to 1.a0.3.2.
- Change the default access name for HTTP/RTSP stream format.

Bugs Fixed:
- Fixed CVE-2019-10256, an authentication bypass vulnerability.
- 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: 2018/12/04
New Feature:
N/A
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.

Release Note

Release Version: 0106a
Date: 2018/08/08
New Feature:
N/A
Changed Feature:
N/A
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 eventscript.cgi.

* 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.