[Statement] Firmware decryption key disclosure

06.13.2025

Hanwha Vision Cybersecurity Team (S-Cert)

Hanwha Vision has become aware of a recently published blog post and videos analyzing the security of a specific Hanwha Vision camera product. Following an internal investigation by Hanwha Vision Cybersecurity Team (S-CERT), we have confirmed that the issue is limited to the following camera models:

- Wisenet 5 based X/T series, Wisenet Q series, Wisenet A series, and older PNM Multi-sensor cameras

We would like to assure our customers that, to date, there have been no reported security breaches or serious data leaks involving these camera products. Below is a summary of our analysis of the video/blog content, the associated risks, and our mitigation approach.

■ Summary of the Published Blog/Video Content

- Analysis of camera firmware using sophisticated and destructive "chip-off + flash memory dump" techniques. The analysis was not performed with the device on a network.
- Exposure of the encryption keys within the firmware.

■ Risk Assessment

- For certain older camera models identified in the videos, it might be possible to modify firmware with a malicious intent. **Note, however, that all Hanwha Vision network devices are protected by password-based access control and modified firmware cannot be installed in the devices without device credentials.**
- This issue is a known and common risk affecting many conventional IoT devices that do not support secure update or secure boot features.

■ Risk Mitigation Measures

- Use **only firmware** distributed through Hanwha Vision's official websites[1] or Wisenet Device Manager Software provided from Hanwha Vision.
- Apply the latest firmware updates to prevent the installation of unauthorized firmware.
- Ensure strong password management for all device administrator passwords.

■ Enhanced Security Measures

[1] Hanwha Vision's official websites are as follows:

a. https://www.hanwhavision.com
b. https://www.hanwhavisionamerica.com
c. https://www.hanwhavisionsupport.com
d. https://www.hanwhavision.eu

- For affected legacy camera models, we are updating the exposed encryption keys and implementing firmware digital signature verification, with which the cameras will reject unauthorized firmware files.
  ※ Please note that this issue does not affect our latest camera models, which already feature digital signature verification.

We remain committed to resolving any and all product security concerns and to safeguarding the trust of our customers. Firmware patches and additional updates will be distributed exclusively through Hanwha Vision's official websites. We strongly encourage all users to download and apply the latest firmware only available on Hanwha Vision's official websites.