Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

March 21, 2018 Hanwha Techwin

Vulnerability Report (CVE-2018-6294 ~ 6303)

1. Vulnerability

. The vulnerabilities found by "Kaspersky Lab" are total 10 CVEs.

. List of the CVE registered vulnerabilities are as below (CVE-2018-6294 ~ 6303).

. Impacted Model: All Hanwha Techwin SmartCams
(https://www.wisenetlife.com/en/product/SmartCam/)

2. Risk Analysis

. Except CVE-2018-6302, the vulnerabilities have been resolved already before the CVE registration.

. Users can easily download or update the latest firmware from the cloud system.
Thus, the level of threat is low.

CVE	Summary	State
CVE-2018-6294	Unsecured way of firmware update in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6295	Unencrypted way of remote control and communications in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6296	An undocumented (hidden) capability for switching the web interface in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6297	Buffer overflow in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6298	Remote code execution in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6299	Authentication bypass in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6300	Remote password change in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6301	Arbitrary camera access and monitoring via cloud in Hanwha Techwin Smartcams	Resolved*1
CVE-2018-6302	Denial of service by blocking of new camera registration on the cloud server in Hanwha Techwin Smartcams	Ongoing
CVE-2018-6303	Denial of service by uploading malformed firmware in Hanwha Techwin Smartcams	Resolved*1

[CVE Vulnerability State]

[1] The resolved vulnerabilities are fixed in the firmware updates released from March.

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

. Only one remaining issue (CVE-2018-6302)

→ The camera itself does not carry the risk of the remaining issue (CVE-2018-6302). It is rather an issue for a new camera being disturbed when trying to register on the server.

3. Plan

. Regardless of the risks of found vulnerabilities, Hanwha Techwin will have security reinforcement by enhancing the camera identification logics.

. Hanwha Techwin promise to work diligently in order to deliver solutions for the remaining vulnerability (CVE-2018-6302) until it is fixed (Currently building an update plan).

. The vulnerabilities of SmartCam will be fixed by phase as soon as possible.

. Also, we will keep updating the vulnerability report until all issues are resolved.