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

2018년 3월 21일, 한화 테크윈

보안 취약점 보고서 (CVE-2018-6294 ~ 6303)

1. 취약점 확인

. "카스퍼스키 연구소(Kaspersky Lab)"에 의해 총 10개의 보안 취약점(CVE)이 발견되었습니다.

. CVE 등록된 취약점 리스트(CVE-2018-6294 ~ 6303)는 아래표와 같습니다.

. 영향 받는 모델: 한화 테크윈의 모든 스마트캠
(https://www.wisenetlife.com/ko/product/SmartCam/)

2. 리스크 분석

. CVE-2018-6302를 제외한 모든 보안 취약점들은 CVE에 등록되기 이전 이미 해결되었습니다.

. 사용자는 최신 펌웨어를 클라우드 시스템으로부터 손쉽게 다운로드 및 업데이트를 할 수가 있기 때문에 보안 위협의 영향도는 매우 낮습니다.

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

[CVE 보안취약점 상태]

1 보안 취약점은 3월 이후부터 배포된 펌웨어 업데이트를 통해 해결되었습니다.

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

. 한가지 미해결 이슈 (CVE-2018-6302)

→ 남아 있는 한가지 이슈(CVE-2018-6302)는 카메라 자체에 위험을 초래하는 사항이 아니며, 신규 카메라가 서버에 등록 시 등록을 방해할 수 있는 서비스 거부 공격에 대한 이슈입니다.

3. 대응 계획

. 한화 테크윈은 발견된 보안 취약점의 위험성에 관계없이 카메라 식별 로직을 더욱 강화하여 보안을 강화할 예정입니다.

. 한화 테크윈은 수정될 때까지 남아 있는 보안 취약점(CVE-2018-6302)에 대한 솔루션을 제공하기 위해 부단히 노력할 것을 약속합니다 (현재 업데이트 계획 수립중).

. 스마트캠의 보안 취약점은 최대한 빨리 단계별로 수정될 예정입니다.

. 또한, 모든 문제가 해결될 때까지 보안 취약점 보고서를 계속 업데이트할 것입니다.